(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－149413

(43)公開日　平成11年(1999)６月２日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ	12/14	３１０Ｚ
	12/00	５３７		12/00	５３７Ｚ

審査請求　未請求　請求項の数29　ＯＬ　（全 35 頁）

(21)出願番号　特願平9－314017

(22)出願日　平成９年(1997)11月14日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　蒲田　順
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　黒田　康嗣
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　小野　越夫
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

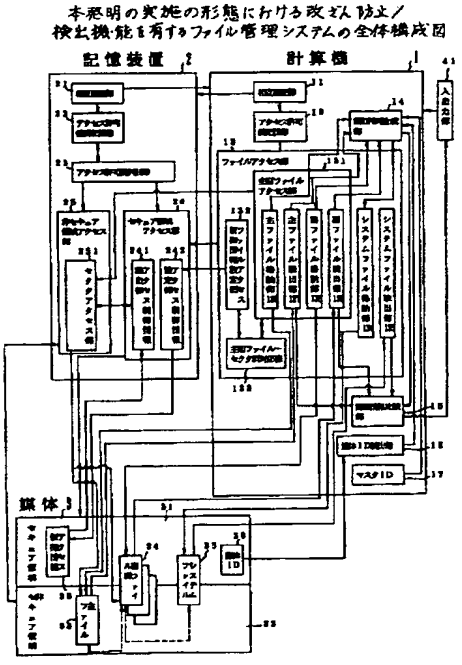
(74)代理人　弁理士　大菅　義之　（外１名）

(54)【発明の名称】　改ざん防止／検出機能を有するファイル管理システム

(57)【要約】

【課題】　電子化されたデータファイルの改ざんを防止することが課題である。

【解決手段】　通常アクセスが許されないセキュア領域に、データファイルから生成した認証子を保存しておくことで、上記データフィルの改ざんを検出することができる。しかも、上記データフィルを主ファイルとし、主ファイルと関連付けられたさまざまな副ファイルから、上記認証子を生成することで、上記認証子を保存しておく上記セキュア領域のサイズは、小さくて済む。



1

【特許請求の範囲】
【請求項１】　計算機と記憶装置とを備えたファイルシステムであって、該計算機は、
該記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、
該アクセス許可鍵を格納するアクセス許可鍵記憶手段と、
該アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、
を備え、
該記憶装置は、
該計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、
該アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、
該ファイルアクセス手段から送付され該アクセス許可鍵記憶手段に格納されたアクセス許可鍵と該アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、
該アクセス許可鍵判別手段が同一と判断した場合、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、
を備えたファイル管理システム。
【請求項２】　請求項１に記載のファイル管理システムであって、
前記計算機に備えられた相互認証手段および前記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システム。
【請求項３】　主ファイルに関連付けられた一つまたは複数の副ファイルを格納する副ファイル格納手段と、
該副ファイルの検証に使用する副ファイル認証情報を生成する認証情報生成手段と、
該副ファイル認証情報を関連付けたシステムファイルを格納するシステムファイル格納手段と、
を備えることを特徴とするファイル管理システム。
【請求項４】　主ファイルを格納する主ファイル格納手段と、
該主ファイルの検証に使用する主ファイル認証情報を生成する認証情報生成手段と、
該主ファイル認証情報を関連付けた少なくとも１つの副ファイルを格納する副ファイル格納手段と、
を備えることを特徴とするファイル管理システム。
【請求項５】　主ファイルを格納する主ファイル格納手段と、
該主ファイル認証情報を関連付けた少なくとも１つの副ファイルを格納する副ファイル格納手段と、
該主ファイルの検証に使用する主ファイル認証情報および該副ファイルの検証に使用する副ファイル認証情報を生成するを生成する認証情報生成手段と、
該副ファイル認証情報を関連付けたシステムファイルを

2

格納するシステムファイル格納手段と、
を備えることを特徴とするファイル管理システム。
【請求項６】　請求項５において、前記主ファイル、前記副ファイルおよび前記システムファイルを通常アクセスできる非セキュア領域に格納することを特徴とするファイル管理システム。
【請求項７】　請求項５において、前記主ファイルを通常アクセスできる非セキュア領域に格納し、前記副ファイルおよび前記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システム。
【請求項８】　請求項５において、前記主ファイルおよび前記副ファイルを通常アクセスできる非セキュア領域に格納し、前記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システム。
【請求項９】　請求項６～８のいずれか１項記載のファイル管理システムであって、
計算機と、
記憶装置とを更に備え、
該計算機は、
該記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、
該アクセス許可鍵を格納するアクセス許可鍵記憶手段と、該アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、
を備え、
該記憶装置は、
該計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、
該アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、該アクセス許可鍵記憶手段に格納されたアクセス許可鍵と該アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、
通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、
を備え、
該認証情報生成手段は、
該相互認証の後、該セキュア領域に格納されている媒体固有の媒体ＩＤを読み出し、該主ファイル認証情報および該副ファイル認証情報の生成に使用することを特徴とするファイル管理システム。
【請求項１０】　請求項９に記載のファイル管理システムであって、
前記計算機に備えられた相互認証手段および前記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システム。
【請求項１１】　請求項９または１０に記載のファイル管理システムであって、

該媒体ＩＤは、カードＩＤであることを特徴とするファイル管理システム。

【請求項１２】　請求項９または１０に記載のファイル管理システムであって、

該媒体ＩＤは、マスタＩＤであることを特徴とするファイル管理システム。

【請求項１３】　請求項９～１２のいずれか１項記載のファイル管理システムであって、

前記認証情報の生成は、ファイルのレコードごとに行うことを特徴とするファイル管理システム。

【請求項１４】　主ファイルに関連付けられた１つまたは複数の副ファイルを読み出す副ファイル読出手段と、

該副ファイル読出手段から読み出された副ファイルから副ファイル認証情報を生成する認証情報生成手段と、

該副ファイルに関連付けられたシステムファイルから副ファイル認証情報を読み出すシステムファイル読出手段と、

該認証情報生成手段が生成した副ファイル認証情報と該システムファイル読出手段が読み出した副ファイル認証情報とを比較する認証情報比較手段と、

備えることを特徴とするファイル管理システム。

【請求項１５】　主ファイルを読み出す主ファイル読出手段と、該主ファイル読出手段から読み出された主ファイルから主ファイル認証情報を生成する認証情報生成手段と、

該主ファイルに関連付けられた副ファイルから主ファイル認証情報を読み出す副ファイル読出手段と、

該認証情報生成手段が生成した主ファイル認証情報と該副ファイル読出手段が読み出した主ファイル認証情報とを比較する認証情報比較手段と、

備えることを特徴とするファイル管理システム。

【請求項１６】　主ファイルを読み出す主ファイル読出手段と、

該主ファイルに関連付けられた副ファイルのうち主ファイル認証情報および該主ファイルに関連付けられた１つまたは複数の副ファイルを読み出す副ファイル読出手段と、

該副ファイルに関連付けられたシステムファイルから副ファイル認証情報を読み出すシステムファイル読出手段と、

該主ファイル読出手段から読み出された主ファイルから主ファイル認証情報を生成し、該副ファイル読出手段から読み出された副ファイルから副ファイル認証情報を生成する認証情報生成手段と、

該認証情報生成手段生成した主ファイル認証情報と該副ファイル読出手段が読み出した主ファイル認証情報とを比較し、該認証情報生成手段生成した副ファイル認証情報と該システムファイル読出手段が読み出した副ファイル認証情報とを比較する認証情報比較手段と、

を備えることを特徴とするファイル管理システム。

【請求項１７】　請求項１６において、前記主ファイル、前記副ファイルおよび前記システムファイルを通常アクセスできる非セキュア領域に格納することを特徴とするファイル管理システム。

【請求項１８】　請求項１６において、前記主ファイルを通常アクセスできる非セキュア領域に格納し、前記副ファイルおよび前記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システム。

【請求項１９】　請求項１６において、前記主ファイルおよび前記副ファイルを通常アクセスできる非セキュア領域に格納し、前記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システム。

【請求項２０】　請求項１７～１９のいずれか１項記載のファイル管理システムであって、

計算機と、

記憶装置とを更に備え、

該計算機は、

該記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、

該アクセス許可鍵を格納するアクセス許可鍵記憶手段と、該アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、

を備え、

該記憶装置は、

該計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、

該アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、

該アクセス許可鍵記憶手段に格納されたアクセス許可鍵と該アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、

通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、

を備え、

該認証情報生成手段は、

該セキュア領域に格納されている媒体固有の媒体ＩＤを該相互認証を行った上で読み出し、該主ファイル認証情報および該副ファイル認証情報の生成に使用することを特徴とするファイル管理システム。

【請求項２１】　請求項２０に記載のファイル管理システムであって、

前記計算機に備えられた相互認証手段および前記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システム。

【請求項２２】　請求項２０または２１に記載のファイル管理システムであって、

該媒体ＩＤは、カードＩＤであることを特徴とするファ

イル管理システム。
【請求項２３】　請求項２０または２１に記載のファイル管理システムであって、
該媒体ＩＤは、マスタＩＤであることを特徴とするファイル管理システム。
【請求項２４】　請求項２０～２３のいずれか１項記載のファイル管理システムであって、
前記認証情報の生成は、ファイルのレコードごとに行うことを特徴とするファイル管理システム。
【請求項２５】　請求項１記載のファイル管理システムであって、
前記セキュア領域アクセス手段は、
前記セキュア領域に格納されたアクセス制御情報を読み出すアクセス制御情報読出手段と、
を更に備え、
前記記憶装置は、該アクセス制御情報に従い主ファイルまたは該主ファイルと関連付けられた副ファイルに対しセクタあるいはセクタ群単位でアクセスするセクタアクセス手段と、をさらに備えることを特徴とするファイル管理システム。
【請求項２６】　請求項２５記載のファイル管理システムであって、
前記セキュア領域アクセス手段は、
前記セキュア領域にアクセス制御情報を設定するアクセス制御情報設定手段をさらに備えることを特徴とするファイル管理システム。
【請求項２７】　請求項９～１３、２０～２４のいずれか１項記載のファイル管理システムであって、前記媒体ＩＤまたは前記カードＩＤまたは前記マスタＩＤのうち、１つまたは２つまたは３つのＩＤを用いて認証情報を生成することを特徴とするファイル管理システム。
【請求項２８】　計算機と記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証工程と、
該アクセス許可鍵を格納するアクセス許可鍵記憶工程と、
該アクセス許可鍵を格納するアクセス許可鍵群記憶工程と、
該アクセス許可鍵とともにアクセス要求を送付するファイルアクセス工程と、
該アクセス許可鍵記憶工程で格納されたアクセス許可鍵と該アクセス許可鍵群記憶工程で格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別工程と、
通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス工程と、
を備えたファイル管理方法。
【請求項２９】　計算機と記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手順と、
該アクセス許可鍵を格納するアクセス許可鍵記憶手順と、
該アクセス許可鍵を格納するアクセス許可鍵群記憶手順と、
該アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手順と、該アクセス許可鍵記憶手順で格納されたアクセス許可鍵と該アクセス許可鍵群記憶手順で格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手順と、
通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手順と、
を備えた機能をコンピュータに実現させるためのファイル管理プログラムを記録したコンピュータ読取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ファイルの改ざん防止および検出機能を有するファイル管理システムに関し、特に、データファイルから間接的に生成した認証子を、操作者がアクセスできない領域に格納することで、ファイルの改ざん防止および検出を可能とするファイル管理システムに関する。
【０００２】
【従来の技術】税務関連帳票等の公文書の電子化が進むにつれ、紙で保存していた時と同様に電子化データを長期間、安全に、証拠能力を保って保存したいというニーズが高まっている。電子化データは、追加、削除、修正あるいはネットワークなどを介しての転送など、加工や再利用が非常に容易である。このため、電子化データは、作成者が作成した通りのものではなく、第三者がデータを改ざんする危険性がある。
【０００３】この問題を解決するため、出願人は、特願平９－８８４８５号（ファイルシステムおよびプログラム記録媒体、平成９年４月７日出願）を出願した。これは、ＯＳ（Operating System）内のファイル管理モジュール（ファイルシステム）と、ユーザには通常アクセスを許さない領域（セキュア領域）を設定できる記憶媒体（セキュア媒体）が連携して、セキュア領域にデータファイルの改ざん検出用の認証子およびデータファイルのアクセスログ等をデータファイルに関連付けて保存しておくことで、不正ユーザの低レベルアクセスによる不正改ざんの検出、また正当ユーザの悪意を持った不正改ざんの検出が行えるファイルシステムである。
【０００４】
【発明が解決しようとする課題】ところが、上記従来例では、通常ユーザによるセキュア領域アクセスをファイルシステムにより守っているため、そのようなファイルシステムを有さないシステムでは容易にセキュア領域がアクセスされ、その結果データファイルに関連付けられた認証子、アクセスログ等が都合のいいように改ざんさ

れてしまう可能性があった。

【０００５】また、アクセスログ等は動的に拡大するため、アクセスの頻度等によって必要なセキュア領域のサイズは異なるが、一般的にセキュア領域と通常の領域のサイズを動的に変更することは難しい。

【０００６】

【課題を解決するための手段】そこで、本発明では、上記従来例の前者の問題に対してはセキュア領域をファイルシステムではなく、ファイルシステムとの間で相互認証の得られた記憶装置の例えばファームウェアで守るという方法をとることで問題を解決する。また、後者の問題に対しては、主ファイルであるデータファイルに関連付けられた認証子やアクセスログ等の副ファイルは通常の領域に置き、上記副ファイルから生成した認証子だけをセキュア領域に置くことで問題解決をはかる。請求項１の発明は、計算機と記憶装置とを備えたファイルシステムであって、上記計算機は、上記記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵記憶手段と、上記アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、を備え、上記記憶装置は、上記計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、上記アクセス許可鍵記憶手段に格納されたアクセス許可鍵と上記アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、を備えたファイル管理システムである。

【０００７】請求項２の発明は、請求項１に記載のファイル管理システムであって、上記計算機に備えられた相互認証手段および上記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システムである。

【０００８】請求項３の発明は、主ファイルに関連付けられた一つまたは複数の副ファイルを格納する副ファイル格納手段と、上記副ファイルの検証に使用する副ファイル認証情報を生成する認証情報生成手段と、上記副ファイル認証情報をシステムファイルとして関連付けて格納するシステムファイル格納手段と、を備えることを特徴とするファイル管理システムである。

【０００９】請求項４の発明は、主ファイルを格納する主ファイル格納手段と、上記主ファイルの検証に使用する主ファイル認証情報を生成する認証情報生成手段と、上記主ファイル認証情報を副ファイルの１つとして関連付けて格納する副ファイル格納手段と、を備えることを特徴とするファイル管理システムである。

【００１０】請求項５の発明は、主ファイルを格納する主ファイル格納手段と、上記主ファイルの検証に使用する主ファイル認証情報を生成する認証情報生成手段と、上記主ファイル認証情報を副ファイルの１つとして関連付けて格納する副ファイル格納手段と、主ファイルに関連付けられた一つまたは複数の副ファイルを格納する副ファイル格納手段と、上記副ファイルの検証に使用する副ファイル認証情報を生成する認証情報生成手段と、上記副ファイル認証情報をシステムファイルとして関連付けて格納するシステムファイル格納手段と、を備えることを特徴とするファイル管理システムである。

【００１１】請求項６の発明は、請求項５において、上記主ファイル、上記副ファイルおよび上記システムファイルを通常アクセスできる非セキュア領域に格納することを特徴とするファイル管理システムである。

【００１２】請求項７の発明は、請求項５において、上記主ファイルを通常アクセスできる非セキュア領域に格納し、上記副ファイルおよび上記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システムである。

【００１３】請求項８の発明は、請求項５において、上記主ファイルおよび上記副ファイルを通常アクセスできる非セキュア領域に格納し、上記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システムである。

【００１４】請求項９の発明は、請求項６～８のいずれか１項記載のファイル管理システムであって、計算機と、記憶装置とを更に備え、上記計算機は、上記記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵記憶手段と、上記アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、を備え、上記記憶装置は、上記計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、上記アクセス許可鍵記憶手段に格納されたアクセス許可鍵と上記アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、を備え、上記認証情報生成手段は、上記セキュア領域に格納されている媒体固有の媒体ＩＤを上記相互認証を行った上で読み出し、上記主ファイル認証情報および上記副ファイル認証情報の生成に使用することを特徴とするファイル管理システムである。

【００１５】請求項１０の発明は、請求項９に記載のファイル管理システムであって、上記計算機に備えられた相互認証手段および上記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システムである。

【００１６】請求項１１の発明は、請求項９または１０に記載のファイル管理システムであって、上記媒体ＩＤ

は、カードＩＤであることを特徴とするファイル管理システムである。

【００１７】請求項１２の発明は、請求項９または１０に記載のファイル管理システムであって、上記媒体ＩＤは、マスタＩＤであることを特徴とするファイル管理システムである。

【００１８】請求項１３の発明は、請求項９～１２のいずれか１項記載のファイル管理システムであって、上記認証情報の生成は、ファイルのレコードごとに行うことを特徴とするファイル管理システムである。

【００１９】請求項１４の発明は、主ファイルに関連付けられた１つまたは複数の副ファイルを読み出す副ファイル読出手段と、上記副ファイル読出手段から読み出された副ファイルから副ファイル認証情報を生成する認証情報生成手段と、上記副ファイルに関連付けられたシステムファイルから副ファイル認証情報を読み出すシステムファイル読出手段と、上記認証情報生成手段生成した副ファイル認証情報と上記システムファイル読出手段が読み出した副ファイル認証情報とを比較する認証情報比較手段と、備えることを特徴とするファイル管理システムである。

【００２０】請求項１５の発明は、主ファイルを読み出す主ファイル読出手段と、上記主ファイル読出手段から読み出された主ファイルから主ファイル認証情報を生成する認証情報生成手段と、上記主ファイルに関連付けられた副ファイルから主ファイル認証情報を読み出す副ファイル読出手段と、上記認証情報生成手段生成した主ファイル認証情報と上記副ファイル読出手段が読み出した主ファイル認証情報とを比較する認証情報比較手段と、備えることを特徴とするファイル管理システムである。

【００２１】請求項１６の発明は、主ファイルを読み出す主ファイル読出手段と、上記主ファイルに関連付けられた１つまたは複数の副ファイルおよび上記主ファイルに関連付けられた副ファイルから主ファイル認証情報を読み出す副ファイル読出手段と、上記副ファイルに関連付けられたシステムファイルから副ファイル認証情報を読み出すシステムファイル読出手段と、上記主ファイル読出手段から読み出された主ファイルから主ファイル認証情報を生成し、上記副ファイル読出手段から読み出された副ファイルから副ファイル認証情報を生成する認証情報生成手段と、上記認証情報生成手段生成した主ファイル認証情報と上記副ファイル読出手段が読み出した主ファイル認証情報とを比較し、上記認証情報生成手段生成した副ファイル認証情報と上記システムファイル読出手段が読み出した副ファイル認証情報とを比較する認証情報比較手段と、備えることを特徴とするファイル管理システムである。

【００２２】請求項１７の発明は、請求項１６において、上記主ファイル、上記副ファイルおよび上記システムファイルを通常アクセスできる非セキュア領域に格納することを特徴とするファイル管理システムである。

【００２３】請求項１８の発明は、請求項１６において、上記主ファイルを通常アクセスできる非セキュア領域に格納し、上記副ファイルおよび上記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システムである。

【００２４】請求項１９の発明は、請求項１６において、上記主ファイルおよび上記副ファイルを通常アクセスできる非セキュア領域に格納し、上記システムファイルを通常アクセスできないセキュア領域に格納することを特徴とするファイル管理システムである。

【００２５】請求項２０の発明は、請求項１７～１９のいずれか１項記載のファイル管理システムであって、計算機と、記憶装置とを更に備え、上記計算機は、上記記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵記憶手段と、上記アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手段と、を備え、上記記憶装置は、上記計算機との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手段と、上記アクセス許可鍵を格納するアクセス許可鍵群記憶手段と、上記アクセス許可鍵記憶手段に格納されたアクセス許可鍵と上記アクセス許可鍵群記憶手段に格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手段と、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手段と、を備え、上記認証情報生成手段は、上記セキュア領域に格納されている媒体固有の媒体ＩＤを上記相互認証を行った上で読み出し、上記主ファイル認証情報および上記副ファイル認証情報の生成に使用することを特徴とするファイル管理システムである。

【００２６】請求項２１の発明は、請求項２０に記載のファイル管理システムであって、上記計算機に備えられた相互認証手段および上記ファイルアクセス手段は、ハードウェアで実現されることを特徴とするファイル管理システムである。

【００２７】請求項２２の発明は、請求項２０または２１に記載のファイル管理システムであって、上記媒体ＩＤは、カードＩＤであることを特徴とするファイル管理システムである。

【００２８】請求項２３の発明は、請求項２０または２１に記載のファイル管理システムであって、上記媒体ＩＤは、マスタＩＤであることを特徴とするファイル管理システムである。

【００２９】請求項２４の発明は、請求項２０～２３のいずれか１項記載のファイル管理システムであって、上記認証情報の生成は、ファイルのレコードごとに行うことを特徴とするファイル管理システムである。

【００３０】請求項２５の発明は、請求項１記載のファ

イル管理システムであって、上記記憶装置は、主ファイルまたは上記主ファイルと関連付けられた副ファイルに対しセクタあるいはセクタ群単位でアクセスするセクタアクセス手段とをさらに備え、上記セキュア領域アクセス手段は、上記セキュア領域に格納されたアクセス制御情報を読み出すアクセス制御情報読出手段と、を備えることを特徴とするファイル管理システムである。

【００３１】請求項２６の発明は、請求項２５記載のファイル管理システムであって、上記セキュア領域アクセス手段は、上記セキュア領域にアクセス制御情報を設定するアクセス制御情報設定手段をさらに備えることを特徴とするファイル管理システムである。

【００３２】請求項２７の発明は、請求項９～１３、２０～２４のいずれか１項記載のファイル管理システムであって、上記媒体ＩＤまたは上記カードＩＤまたは上記マスタＩＤのうち、１つまたは２つまたは３つのＩＤを用いて認証情報を生成することを特徴とするファイル管理システムである。

【００３３】請求項２８の発明は、計算機と記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証工程と、上記アクセス許可鍵を格納するアクセス許可鍵記憶工程と、上記アクセス許可鍵とともにアクセス要求を送付するファイルアクセス工程と、上記アクセス許可鍵を格納するアクセス許可鍵群記憶工程と、上記アクセス許可鍵記憶工程で格納されたアクセス許可鍵と上記アクセス許可鍵群記憶工程で格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別工程と、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス工程と、を備えたファイル管理方法である。

【００３４】請求項２９の発明は、計算機と記憶装置との間で相互認証を行い相互認証された場合はアクセス許可鍵を生成する相互認証手順と、上記アクセス許可鍵を格納するアクセス許可鍵記憶手順と、上記アクセス許可鍵とともにアクセス要求を送付するファイルアクセス手順と、上記アクセス許可鍵を格納するアクセス許可鍵群記憶手順と、上記アクセス許可鍵記憶手順で格納されたアクセス許可鍵と上記アクセス許可鍵群記憶手順で格納されたアクセス許可鍵とが同一かどうかを判別するアクセス許可鍵判別手順と、通常ではアクセスできないセキュア領域にアクセスするセキュア領域アクセス手順と、を備えた機能をコンピュータに実現させるためのファイル管理プログラムを記録したコンピュータ読取り可能な記録媒体である。

【００３５】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態について詳細に説明する。図１は、本発明の実施の形態における改ざん防止／検出機能を有するファイル管理システムの全体構成図である。

【００３６】各構成部は、図４、図６、図８、図１０、

図１２、図１４、図１５、図１６、図１８、図２０、図２２、図２４、図２５、図２６、図２８、および図３０を用いて各実施の形態を説明しながら後述する。

【００３７】なお、計算機１側の相互認証部１１、認証情報生成部１４および認証情報比較部１５等の各構成部は、それぞれ、ＯＳ内のファイル管理モジュール内におけるソフトウェアサブルーチンであっても良いし、ハードウェアにより構成されていても良い。

【００３８】図２は、本発明の実施の形態におけるファイルの構成を説明するための図である。主ファイルから生成された認証子は副ファイルに格納され、副ファイルから生成された認証子はシステムフィルに格納される。

【００３９】図３は、ＭＡＣの計算方法を説明するための図である。主ファイルや副ファイルなどの元データを例えば６４ｂｉｔずつに分割し、暗号化する。暗号化された値と次の６４ｂｉｔとの排他的論理和をとり、これをまた暗号化する。それぞれの暗号化により得られた値あるいはその値のうちの一部、例えば上位３２ｂｉｔを認証子とする事もできるが、後述する各実施の形態においては、この処理を最後まで繰り返し、最終的に得られた値の上位３２ｂｉｔを認証子とする。

【００４０】図４は、本発明の第１の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図５は、本発明の第１の実施の形態における動作フローチャートである。

【００４１】ステップＳ５１で、計算機１側の相互認証部１１と記憶装置２側の相互認証部２１は、計算機１および記憶装置２の双方の間で相互認証を行う。ステップＳ５２で、相互認証に成功したら、ステップ５３で、共通のアクセス許可鍵を生成する。ステップＳ５４で、計算機１側の相互認証部１１は、生成したアクセス許可鍵をアクセス許可鍵記憶部１２に渡し格納する。また、記憶装置２側の相互認証部２１は、生成したアクセス許可鍵をアクセス許可鍵群記憶部２２に渡し格納する。相互認証の方法は、例えば一般的な公開鍵を用いたものにする。

【００４２】ステップＳ５５で、ファイルアクセス部１３は、記憶装置２を介してアクセスする媒体３上のセキュア領域３１にアクセスする場合に、記憶装置２のセキュア領域アクセス部２４に対し、アクセス要求とともにアクセス許可鍵を送付する。

【００４３】ステップＳ５６で、アクセス許可鍵判別部２３は、セキュア領域アクセス部２４に対するファイルアクセス部１３からのアクセス要求とともに送付されたアクセス許可鍵と同一のアクセス許可鍵が、アクセス許可鍵記憶部２２内に存在するかどうかを判別する。存在すれば、ステップＳ５７で、セキュア領域アクセス部２４は、セキュア領域３１へのアクセスを行う。

【００４４】なお、計算機１側の相互認証部１１およびファイルアクセス部１３は、それぞれ、ＯＳ内のファイ

ル管理モジュール内におけるソフトウェアサブルーチンであっても良いし、ハードウェアにより構成されていても良い。

【００４５】図６は、本発明の第２の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図７は、本発明の第２の実施の形態における動作フローチャートである。

【００４６】ステップＳ７１で、副ファイル格納部１３８は、媒体３に副ファイル３４をブロック単位に格納するとともに、後述するステップＳ７４の処理から戻ってきた場合、すなわち、他に副ファイル３４が存在すれば読み出し、今格納しようとしている副ファイル３４と結合して認証情報生成部１４に渡す。

【００４７】ステップＳ７２で、認証情報生成部１４は、結合された副ファイル群３４から認証情報である認証子を生成し、システムファイル格納部１３４に渡す。ステップＳ７３で、副ファイル３４の終端に達したかどうかを見て、終端に達していなければ、ステップＳ７１に戻り、副ファイル３４の次のブロックを処理する。

【００４８】ステップＳ７３で、複数ある副ファイル３４の全ての副ファイル３４について処理したかどうかを見て、処理していない副ファイル３４があれば、ステップＳ７１に戻り、次の副ファイル３４を処理する。

【００４９】ステップＳ７４で、システムファイル格納部１３４は、主ファイル３３および副ファイル群３４を一意に識別できるなんらかのＩＤと認証情報である認証子とをセットにして、システムファイル３５中に格納する。

【００５０】図８は、本発明の第３の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図９は、本発明の第３の実施の形態における動作フローチャートである。

【００５１】ステップ９１で、主ファイル格納部１３６は、媒体３に主ファイル３３をブロック単位に格納するとともに、主ファイル３３を認証情報生成部１４にも渡す。ステップ９２で、これを受け取った認証情報生成部１４は、認証情報である認証子を生成し、副ファイル格納部１３８に渡す。ステップＳ９３で、主ファイル３３の終端に達したかどうかを見て、終端に達していなければ、ステップＳ９１に戻り、主ファイル３３の次のブロックを処理する。

【００５２】ステップＳ９４で、副ファイル格納部１３８は、主ファイル３３を一意に識別できるなんらかのＩＤと認証情報である認証子とをセットにし特定の副ファイル３４中に格納する。図１０は、本発明の第４の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図１１は、本発明の第４の実施の形態における動作フローチャートである。

【００５３】ステップＳ１１１で、主ファイル格納部１３６は、媒体３に主ファイル３３をブロック単位に格納

を行うとともに、認証情報生成部１４に主ファイル３３を渡す。

【００５４】ステップＳ１１２で、認証情報生成部１４は、主ファイル３３から認証情報である認証子を生成し、副ファイル格納部１３８に渡す。ステップＳ１１３で、主ファイル３３の終端に達したかどうかを見て、終端に達していなければ、ステップＳ１１１に戻り、主ファイル３３の次のブロックを処理する。

【００５５】ステップＳ１１４で、副ファイル格納部１３８は、主ファイル３３を一意に識別できるなんらかのＩＤと認証情報である認証子とをセットし、特定の副ファイル３４に格納する。

【００５６】次に、ステップ１１５で、副ファイル読出部１３９は、副ファイル群３４を読み出し、認証情報生成部１４に渡す。ステップ１１６で、認証情報生成部１４は、認証情報である認証子を生成し、システムファイル格納部１３４に渡す。ステップＳ１１７で、副ファイル３４の終端に達したかどうかを見て、終端に達していなければ、ステップＳ１１５に戻り、副ファイル３４の次のブロックを処理する。

【００５７】ステップＳ１１８で、複数ある副ファイル３４の全ての副ファイル３４について処理したかどうかを見て、処理していない副ファイル３４があれば、ステップＳ１１５に戻り、次の副ファイル３４を処理する。全副ファイルの処理が実行される事により、副ファイル読出部１３９は、副ファイル群３４をすべて読み出し、認証情報生成部１４に渡したことになる。

【００５８】ステップＳ１１９で、システムファイル格納部１３４は、主ファイル３３および副ファイル３４を一意に識別できるなんらかのＩＤと認証情報である認証子とをセットにして、システムファイル３５に格納する。なお、主ファイル３３は、非セキュア領域３２に格納されているが、副ファイル３４およびシステムファイル３５は、セキュア領域３１に格納されていても非セキュア領域３２に格納されていても良い。つまり、実データである主ファイル３３は、通常アクセスできる非セキュア領域３２に格納されている必要があり、直接アクセスする必要のない副ファイル３４およびシステムファイル３５は、直接的にはアクセスしないので、セキュア領域３１に格納されていても非セキュア領域３２に格納されていても良い。

【００５９】図１２は、本発明の第５の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図１３は、本発明の第５の実施の形態における動作フローチャートである。

【００６０】第１の実施の形態で説明した相互認証は、予め行っておく。ステップ１３０で、媒体ＩＤ読出部１６は、媒体３上のセキュア領域３１から媒体ＩＤ３６を読み出し、認証情報生成部１４に渡す。

【００６１】ステップ１３１で、主ファイル格納部１３

６は、媒体３に主ファイル３３をブロック単位に格納するとともに、認証情報生成部１４にも主ファイル３３を渡す。

【００６２】ステップ１３２で、認証情報生成部１４は、渡された主ファイル３３から媒体ＩＤ３６を鍵として認証情報である認証子を生成し、副ファイル格納格納部１３８に渡す。ここではＤＥＳ－ＭＡＣを使用し認証子を生成することにする。

【００６３】ステップＳ１３３で、主ファイル３３の終端に達したかどうかを見て、終端に達していなければ、ステップＳ１３１に戻り、主ファイル３３の次のブロックを処理する。

【００６４】ステップＳ１３４で、副ファイル格納部１３８は、主ファイル３３を一意に識別できるなんらかのＩＤと認証情報である認証子とをセットにして、特定の副ファイル３４中に格納する。

【００６５】次に、ステップＳ１３５で、副ファイル読出部１３９は、副ファイルを読み出し、認証情報生成部１４に渡す、さらに、後述するステップＳ１３８の処理から戻ってきた場合、上述のステップＳ１３４で格納したデータを結合し認証情報生成部14に渡す。すなわち、副ファイル群３４をすべて読み出し、今格納した全てを結合し認証情報生成部１４に渡すことになる。

【００６６】ステップＳ１３６で、認証情報生成部１４は、上述と同様に認証情報である認証子を生成し、システムファイル格納部１３４に渡す。ステップＳ１３７で、副ファイル３４の終端に達したかどうかを見て、終端に達していなければ、ステップＳ１３５に戻り、副ファイル３４の次のブロックを処理する。

【００６７】ステップＳ１３８で、複数ある副ファイル３４の全ての副ファイル３４について処理したかどうかを見て、処理していない副ファイル３４があれば、ステップＳ１３５に戻り、次の副ファイル３４を処理する。

【００６８】ステップＳ１３９で、システムファイル格納部１３４は、主ファイル３３および副ファイル群３４を一意に識別できるなんらかのＩＤと認証情報をセットにし、システムファイル３５中に格納する。

【００６９】なお、認証子生成時の鍵として用いる媒体ＩＤ３６は、予め媒体３より読み込んでおいても良い。さらに、主ファイル３３および副ファイル３４は、これらを構成するレコードごとに、上述のような処理を行っても良い。

【００７０】図１４は、本発明の第６の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図１２を用いて説明した第５の実施の形態における媒体ＩＤ読出部１６が読み出す媒体ＩＤ３６が、カードＩＤ１８に代わっているだけで、その他の構成および基本的な動作は同じである。

【００７１】図１５は、本発明の第７の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図１２を用いて説明した第５の実施の形態における媒体ＩＤ読出部１６が読み出す媒体ＩＤ３６が、複数のハードウェアで共通であるマスタＩＤ１７に代わっているだけで、その他の構成および基本的な動作は同じである。

【００７２】図１６は、本発明の第８の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図１７は、本発明の第８の実施の形態における動作フローチャートである。

【００７３】ステップＳ１７１で、上位層（ユーザ等）から入出力部４１を介して検証要求が発生した場合、システムファイル読出部１３５は、システムファイル３５中より対応する認証情報である認証子を読み出し、認証情報比較部１５に渡す。

【００７４】一方、ステップＳ１７２で、副ファイル読出部１３９は、副ファイル３４をブロック単位に読み出し、認証情報生成部１４に渡す。ステップＳ１７３で、認証情報生成部１４は、認証情報である認証子を生成し、認証情報比較部１５に渡す。

【００７５】ステップＳ１７４で、副ファイル３４の終端に達したかどうかを見て、終端に達していなければ、ステップＳ１７２に戻り、副ファイル３４の次のブロックを処理する。

【００７６】ステップＳ１７５で、複数ある副ファイル３４の全ての副ファイル３４について処理したかどうかを見て、処理していない副ファイル３４があれば、ステップＳ１７２に戻り、次の副ファイル３４を処理する。

【００７７】ステップＳ１７６で、認証情報比較部１５は、これらの認証情報である認証子を比較し、同じであれば検証成功、同じでなければ検証失敗を上位層に通知する。

【００７８】図１８は、本発明の第９の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図１９は、本発明の第９の実施の形態における動作フローチャートである。

【００７９】ステップＳ１９１で、上位層（ユーザ等）から入出力部４１を介して検証要求が発生した場合、副ファイル読出部１３９は、特定の副ファイル３４中より対応する認証情報である認証子を読み出し、認証情報比較部１５に渡す。

【００８０】一方、ステップＳ１９２で、主ファイル読出部１３７は、主ファイル３３をブロック単位に読み出し、認証情報生成部１４に渡す。ステップＳ１９３で、認証情報生成部１４は、認証情報である認証子をブロック単位に生成し、認証情報比較部１５に渡す。

【００８１】ステップＳ１９４で、主ファイル３３の終端に達したかどうかを見て、終端に達していなければ、ステップＳ１９２に戻り、主ファイル３３の次のブロックを処理する。

【００８２】ステップＳ１９５で、認証情報比較部１５

は、これらの認証情報である認証子を比較し、同じであれば検証成功、同じでなければ検証失敗を上位層に通知する。

【００８３】図２０は、本発明の第１０の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図２１は、本発明の第１０の実施の形態における動作フローチャートである。

【００８４】ステップＳ２１０で、主ファイル３３の読み出し要求が発行されると、まずシステムファイル読出部１３５が、対応する認証情報である認証子をシステムファイル３５から読み出し、認証情報比較部１５に渡す。

【００８５】一方、ステップＳ２１１で、副ファイル読出部１３９が、副ファイル３４ブロック単位に読み出し、認証情報生成部１４に渡す。ステップＳ２１２で、認証情報生成部１４は、これらから認証情報である認証子をブロック単位に再生成し、認証情報比較部１５に渡す。

【００８６】ステップＳ２１３で、副ファイル３４の終端に達したかどうかを見て、終端に達していなければ、ステップＳ２１１に戻り、副ファイル３４の次のブロックを処理する。

【００８７】ステップＳ２１４で、複数ある副ファイル３４の全ての副ファイル３４について処理したかどうかを見て、処理していない副ファイル３４があれば、ステップＳ２１１に戻り、次の副ファイル３４を処理する。

【００８８】ステップＳ２１５で、認証情報比較部１５は、これらの認証情報である認証子と再生成した認証情報である認証子とを比較し、同じでなければ検証失敗を上位層に通知する。

【００８９】次に、ステップＳ２１６で、副ファイル読出部１３９は、副ファイル３４から主ファイル３３の認証情報である認証子を読み出し、認証情報比較部１５に渡す。

【００９０】一方、ステップＳ２１７で、主ファイル読出部１３７は、主ファイル３３をブロック単位に読み出し、認証情報生成部１４に渡す。ステップＳ２１８で、認証情報生成部１４は、ブロック単位に認証情報である認証子を再生成し、認証情報比較部１５に渡す。

【００９１】ステップＳ２１９で、主ファイル３３の終端に達したかどうかを見て、終端に達していなければ、ステップＳ２１７に戻り、主ファイル３３の次のブロックを処理する。

【００９２】ステップＳ２２０で、認証情報比較部１５は、読み出した認証情報である認証子と再生成した認証情報である認証子とを比較し、検証結果を上位層に通知する。

【００９３】なお、主ファイル３３は、非セキュア領域に格納されているが、副ファイル３４およびシステムファイル３５は、セキュア領域に格納されていても非セキュア領域に格納されていても良い。

【００９４】図２２は、本発明の第１１の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図２３は、本発明の第１１の実施の形態における動作フローチャートである。

【００９５】上位層（ユーザ等）から入出力部４１を介して検証要求が発生した場合、ステップＳ２３０で、媒体ＩＤ読出部１６は、媒体３上のセキュア領域３１から媒体ＩＤ３６を読み出し、認証情報生成部１４に渡す。

【００９６】ステップＳ２３１で、システムファイル読出部１３５は、システムファイル３５中より対応する認証情報である認証子を読み出し、認証情報比較部１５に渡す。

【００９７】ステップＳ２３２で、副ファイル読出部１３９は、副ファイル３４をブロック単位に読み出し、認証情報生成部１４に渡す。ステップＳ２３３で、認証情報生成部１４は、媒体ＩＤ３６を鍵として認証情報である認証子を生成し、認証情報比較部１５に渡す。ステップＳ２３４で、副ファイル３４の終端に達したかどうかを見て、終端に達していなければ、ステップＳ２３２に戻り、副ファイル３４の次のブロックを処理する。

【００９８】ステップＳ２３５で、複数ある副ファイル３４の全ての副ファイル３４について処理したかどうかを見て、処理していない副ファイル３４があれば、ステップＳ２３２に戻り、次の副ファイル３４を処理する。

【００９９】ステップＳ２３６で、認証情報比較部１５は、これらの認証情報である認証子と再生成した認証情報である認証子とを比較し、同じでなければ検証失敗を上位層に通知し、終了する。

【０１００】次に、検証に成功した場合、ステップＳ２３７で、副ファイル読出部１３９は、特定の副ファイル３４より認証情報である認証子を読み出し、認証情報比較部１５に渡す。

【０１０１】ステップＳ２３８で、主ファイル読出部が１３７は、主ファイル３３をブロック単位に読み出し、認証情報生成部１４に渡す。ステップＳ２３９で、認証情報生成部１４は、媒体ＩＤ３６を鍵として認証情報である認証子をブロック単位に生成し、認証情報比較部１５に渡す。

【０１０２】ステップＳ２４０で、主ファイル３３の終端に達したかどうかを見て、終端に達していなければ、ステップＳ２３８に戻り、主ファイル３３の次のブロックを処理する。

【０１０３】ステップＳ２４１で、認証情報比較部１５は、これらの認証情報である認証子を比較し、同じであれば検証成功を、同じでなければ検証失敗を上位層に通知し、終了する。

【０１０４】なお、認証子生成時の鍵として用いる媒体ＩＤ３６は、予め媒体３より読み込んでおいても良い。さらに、主ファイル３３および副ファイル３４は、これ

らを構成するレコードごとに、上述のような処理を行っても良い。

【０１０５】図２４は、本発明の第１２の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図２２を用いて説明した第１１の実施の形態における媒体ＩＤ読出部１６が読み出す媒体ＩＤ３６が、カードＩＤ１８に代わっているだけで、その他の構成および基本的な動作は同じである。

【０１０６】図２５は、本発明の第１３の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図２２を用いて説明した第１１の実施の形態における媒体ＩＤ読出部１６が読み出す媒体ＩＤ３６が、複数のハードウェアで共通であるマスタＩＤ１７に代わっているだけで、その他の構成および基本的な動作は同じである。

【０１０７】図２６は、本発明の第１４の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図２７は、本発明の第１４の実施の形態における動作フローチャートである。

【０１０８】ステップＳ２７１で、アクセス制御情報設定部２４２は、アクセス制御情報３８を設定あるいは設定の更新をする。設定時のポリシーとしては様々なものが考えられるが、例えば一旦ライト不可能にすると二度とライト可能にはできないというものも考えられる。

【０１０９】ステップＳ２７２で、セキュア領域３１に存在するアクセス制御情報３８をアクセス制御情報読出部２４１を通じて読み出し、許可されていないアクセスであれば拒絶を通知する。

【０１１０】許可されていれば、ステップＳ２７３で、セクタアクセス部２５１は、アクセス（リード／ライト）要求を受け、記憶媒体３上の非セキュア領域３２内の主ファイル３３および副ファイル３４により構成されるセクタ（群）にアクセスする。

【０１１１】図２８は、本発明の第１５の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図２９は、本発明の第１４の実施の形態における動作フローチャートである。

【０１１２】ステップＳ２９１で、アクセス制御情報設定部１３２は、上位層から指定されたファイルを主副ファイルーセクタ群対応表１３３によりセクタリストに変換し、読み出し専用／書き込み専用／読み書き許可等のアクセスモードと共に記憶装置２内のアクセス制御情報設定部２４２に送る。

【０１１３】ステップＳ２９２で、記憶装置２内のアクセス制御情報設定部２４２は、媒体３上に記憶されているアクセス制御情報３８とその設定ポリシに従い、設定あるいは設定を更新する。この時のポリシとしては、例えば一旦ライト禁止に設定したセクタは二度とライト可能に設定しない等である。

【０１１４】ステップＳ２９３で、主副ファイルアクセス部１３１は、アクセスしたい主ファイル３３および副ファイル３４を主副ファイルーセクタ群対応表１３３に従ってセクタ（群）に変換し、セクタアクセス部２５１に要求を出す。

【０１１５】ステップＳ２９４で、セクタアクセス部２５１は、アクセス制御情報読出部２４１を通じて読み出したアクセス制御情報３８に従ってセクタアクセスの実行／拒絶を行う。

【０１１６】図３０は、本発明の第１６の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。図１２を用いて説明した第５の実施の形態、図１４を用いて説明した第６の実施の形態、図１５を用いて説明した第７の実施の形態、図２２を用いて説明した第１１の実施の形態、図２４を用いて説明した第１２の実施の形態、および図２５を用いて説明した第１３の実施の形態における、媒体ＩＤ３６、カードＩＤ１８、およびマスタＩＤ１７のうち、任意の１つまたは２つまたは３つの組み合わせを用いることもできる。

【０１１７】この際、例えば、媒体ＩＤ３６の一部にロッド番号を現す情報が入っており、特定のロットは長期保存に適した素材、あるいは入念にサーフェースチェックが行われたものであるとする。

【０１１８】公文書は長期間保存する必要があるため、媒体挿入時にファイルシステムが媒体ＩＤ３６を読み出し、上記の特定のロットに含まれない媒体である場合に使用できない旨をユーザに通知する。

【０１１９】なお、本発明の機能が実行されるのであれば、単体の装置であっても、複数の装置からなるシステムあるいは統合装置であっても、ＬＡＮ等のネットワークを介して処理が行なわれるシステムであっても本発明を適用できることは言うまでもない。

【０１２０】また、本発明は、図３１に示すように、バス３１９に接続されたＣＰＵ３１１、ＲＯＭやＲＡＭ３１２、入力装置３１３、出力装置３１４、外部記憶装置３１５、媒体駆動装置、３１６、可搬記録媒体３１９、ネットワーク接続装置３１７で構成されるシステムでも実現できる。すなわち、前述してきた各実施形態のシステムを実現するソフトウェアのプログラムコードを記録したＲＯＭやＲＡＭ３１２、外部記憶装置３１５、可搬記録媒体３１９を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵ３１１やＭＰＵ）がプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【０１２１】この場合、読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記録した可搬記録媒体３１９等は本発明を構成することになる。

【０１２２】プログラムコードを供給するための可搬記録媒体３１９としては、例えば、フロッピーディスク、

ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリーカード、ＲＯＭカード、電子メールやパソコン通信等のネットワーク接続装置３１７（言い換えれば、通信回線）を介して記録した種々の記録媒体などを用いることができる。

【０１２３】また、コンピュータが読み出したプログラムコードを実行することによって、前述した実施形態の機能が実現される他、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳなどが実際の処理の一部または全部を行ない、その処理によっても前述した実施形態の機能が実現される。

【０１２４】さらに、読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリーに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行ない、その処理によっても前述した実勢形態の機能が実現され得る。

【０１２５】

【発明の効果】以上説明してきたように、本発明は、通常ユーザによるセキュア領域アクセスを記憶装置の例えばファームウェアで守っているため、セキュア領域がアクセスされず、その結果データファイルに関連付けられた認証子、アクセスログ等が改ざんされない。

【０１２６】また、データファイルに関連付けられた認証子やアクセスログを通常の領域である非セキュア領域に置き、これらの認証子だけをセキュア領域に置くことでセキュア領域のサイズを小さくできる。

【図面の簡単な説明】

【図１】本発明の実施の形態における改ざん防止／検出機能を有するファイル管理システムの全体構成図である。

【図２】本発明の実施の形態におけるファイルの構成を説明するための図である。

【図３】ＭＡＣの計算方法を説明するための図である。

【図４】本発明の第１の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図５】本発明の第１の実施の形態における動作フローチャートである。

【図６】本発明の第２の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図７】本発明の第２の実施の形態における動作フローチャートである。

【図８】本発明の第３の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図９】本発明の第３の実施の形態における動作フローチャートである。

【図１０】本発明の第４の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図１１】本発明の第４の実施の形態における動作フローチャートである。

【図１２】本発明の第５の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図１３】本発明の第５の実施の形態における動作フローチャートである。

【図１４】本発明の第６の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図１５】本発明の第７の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図１６】本発明の第８の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図１７】本発明の第８の実施の形態における動作フローチャートである。

【図１８】本発明の第９の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図１９】本発明の第９の実施の形態における動作フローチャートである。

【図２０】本発明の第１０の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図２１】本発明の第１０の実施の形態における動作フローチャートである。

【図２２】本発明の第１１の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図２３】本発明の第１１の実施の形態における動作フローチャートである。

【図２４】本発明の第１２の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図２５】本発明の第１３の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図２６】本発明の第１４の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図２７】本発明の第１４の実施の形態における動作フローチャートである。

【図２８】本発明の第１５の実施の形態における改ざん

23　　24

防止／検出機能を有するファイル管理システムの構成図である。

【図２９】本発明の第１４の実施の形態における動作フローチャートである。

【図３０】本発明の第１６の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図である。

【図３１】改ざん防止／検出システムの構成図である。

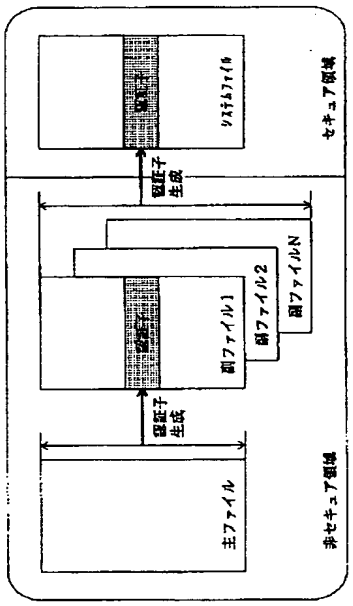
【符号の説明】

１　計算機
２　記憶装置
３　媒体
１１　相互認証部
１２　アクセス許可鍵記憶部
１３　ファイルアクセス部
１４　認証情報生成部
１５　認証情報比較部
１６　媒体ＩＤ読出部
１７　マスタＩＤ
１８　カードＩＤ
２１　相互認証部
２２　アクセス許可鍵群記憶部
２３　アクセス許可鍵判別部
＊２４　セキュア領域アクセス部
２５　非セキュア領域アクセス部
３１　セキュア領域
３２　非セキュア領域
３３　主ファイル
３４　副ファイル（群）
３５　システムファイル
３６　媒体ＩＤ
３８　アクセス制御情報
４１　入出力手段
１３１　主副ファイルアクセス部
１３２　ファイルアクセス制御情報設定部
１３３　主副ファイル－セクタ群対応表
１３４　システムファイル格納部
１３５　システムファイル読出部
１３６　主ファイル格納部
１３７　主ファイル読出部
１３８　副ファイル格納部
１３９　副ファイル読出部
２４１　アクセス制御情報読出部
２４２　アクセス制御情報設定部
２５１　セクタアクセス部

＊

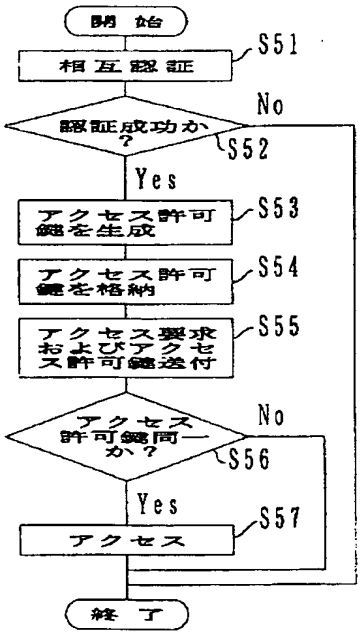
【図２】

本発明の実施の形態における
ファイルの構成を説明するため図



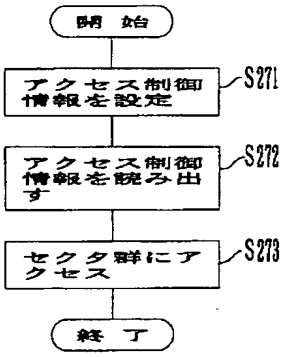
【図５】

本発明の第1の実施の形態における動作フローチャート



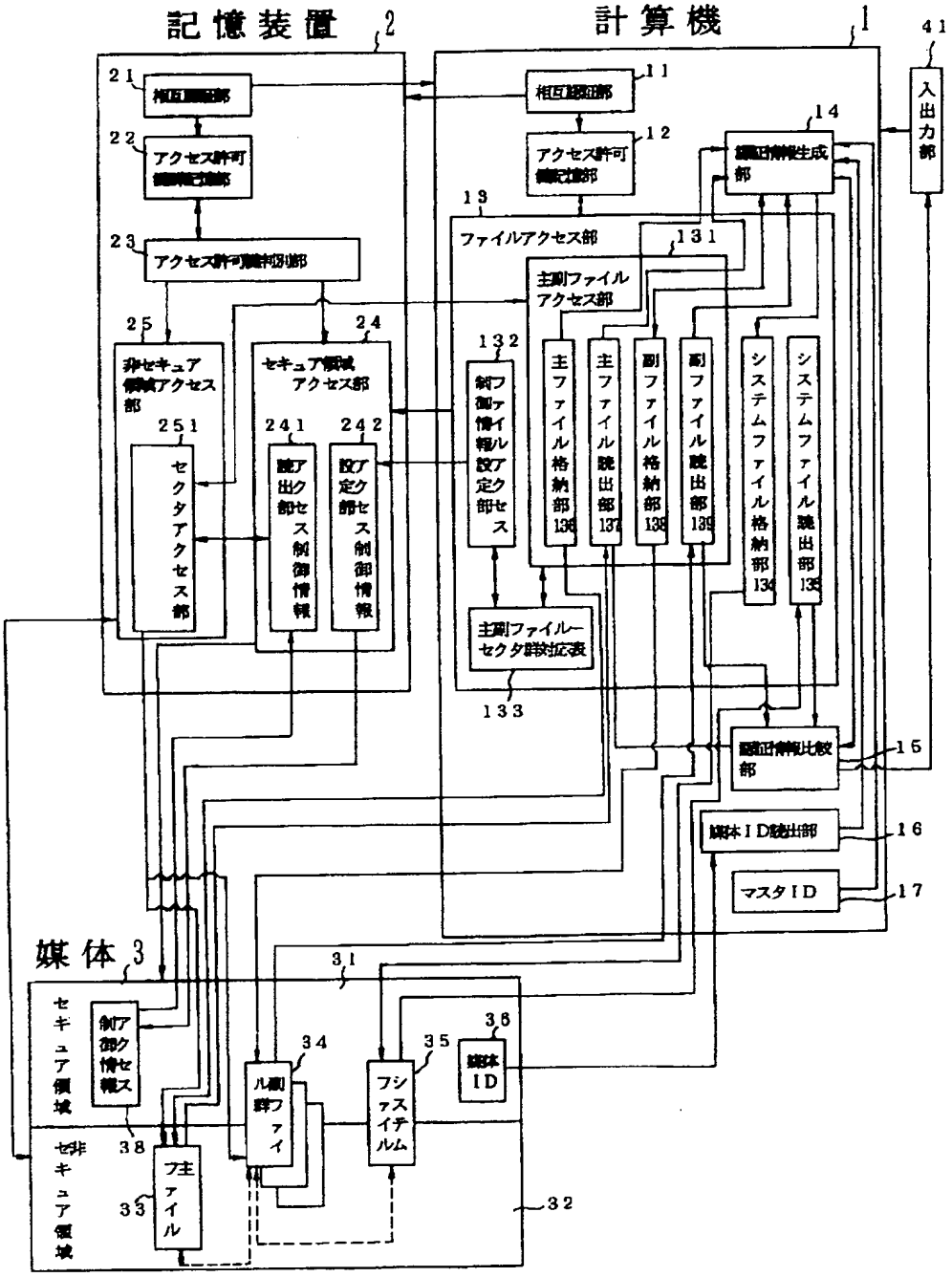
【図２７】

本発明の第１４の実施の形態における
動作フローチャート



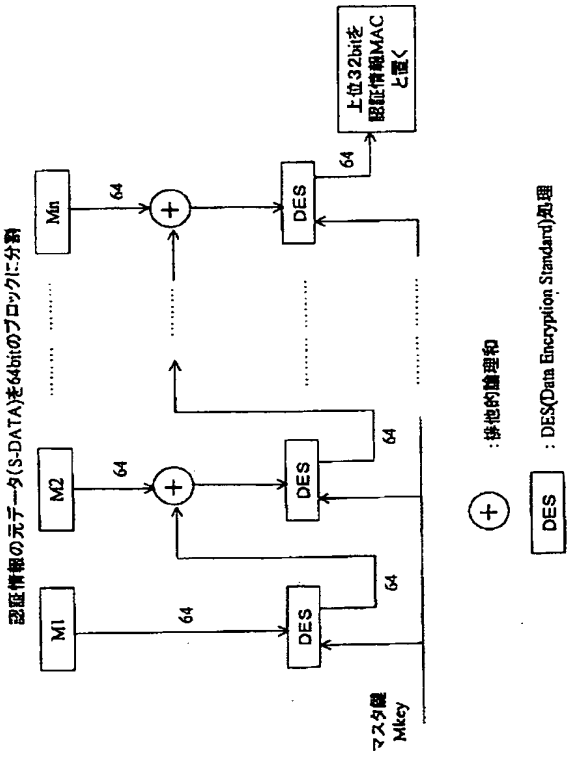
【図１】

本発明の実施の形態における改ざん防止／検出機能を有するファイル管理システムの全体構成図



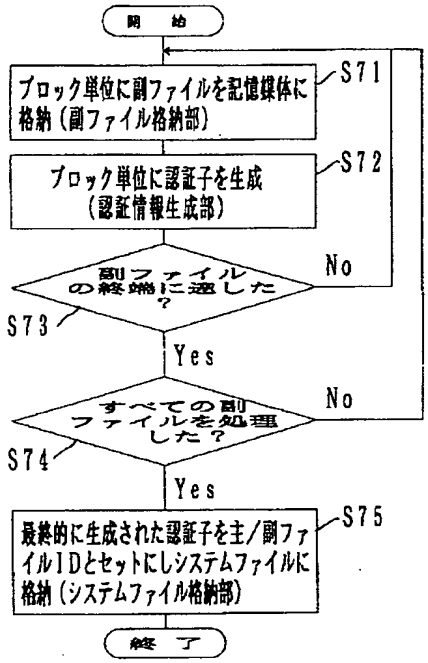
【図３】

MACの計算方法を説明するための図



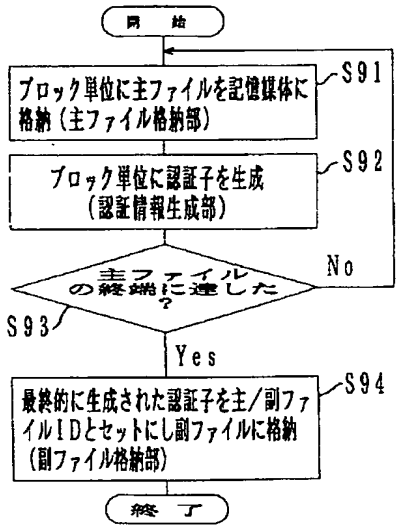
【図７】

本発明の第２の実施の形態における動作フローチャート



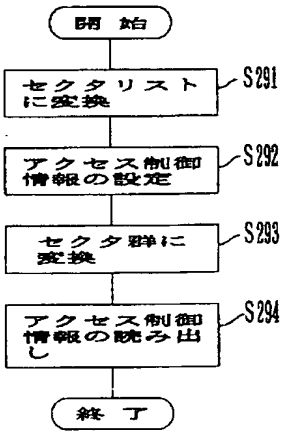
【図９】

本発明の第3の実施の形態における動作フローチャート



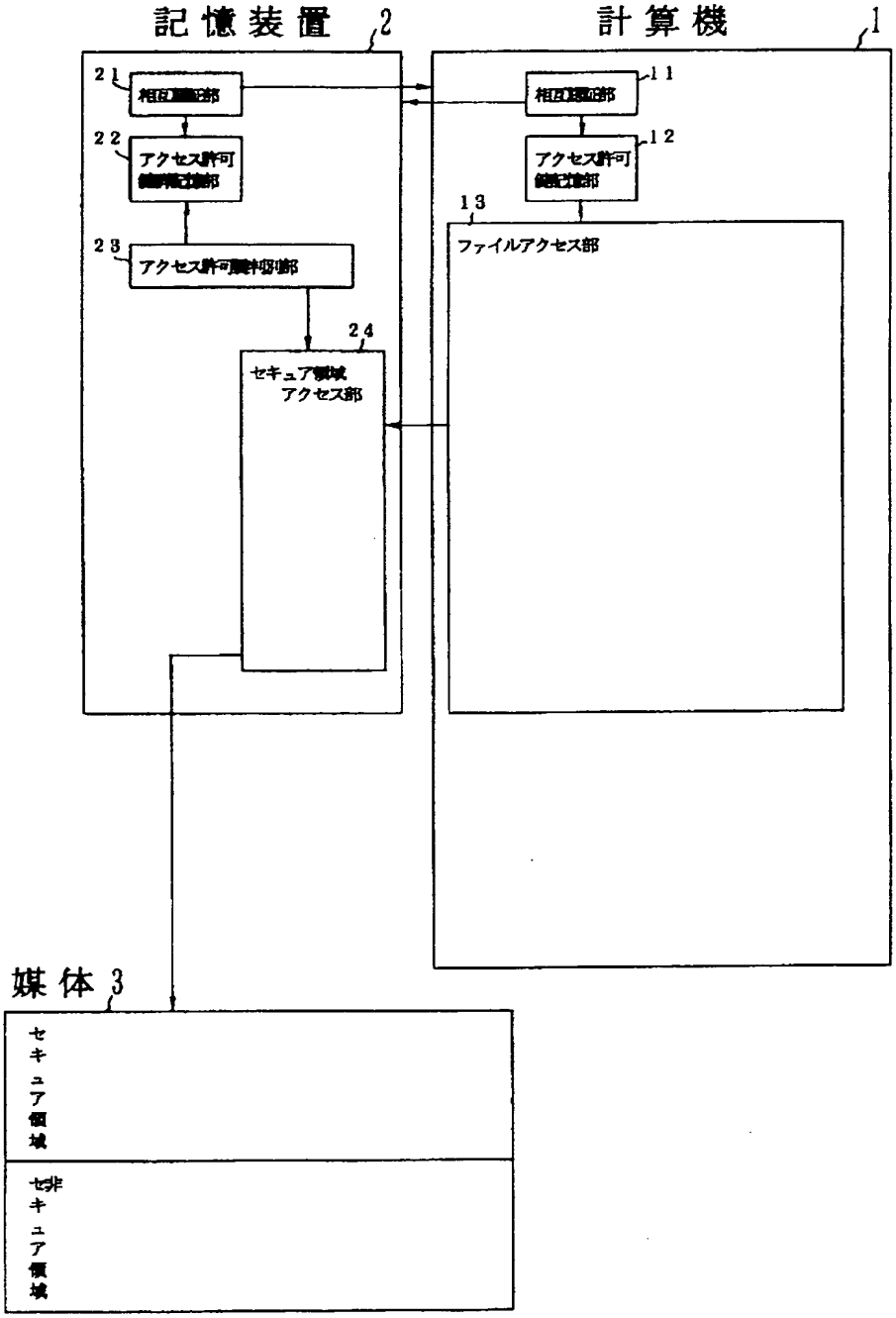
【図２９】

本発明の第１４の実施の形態における動作フローチャート



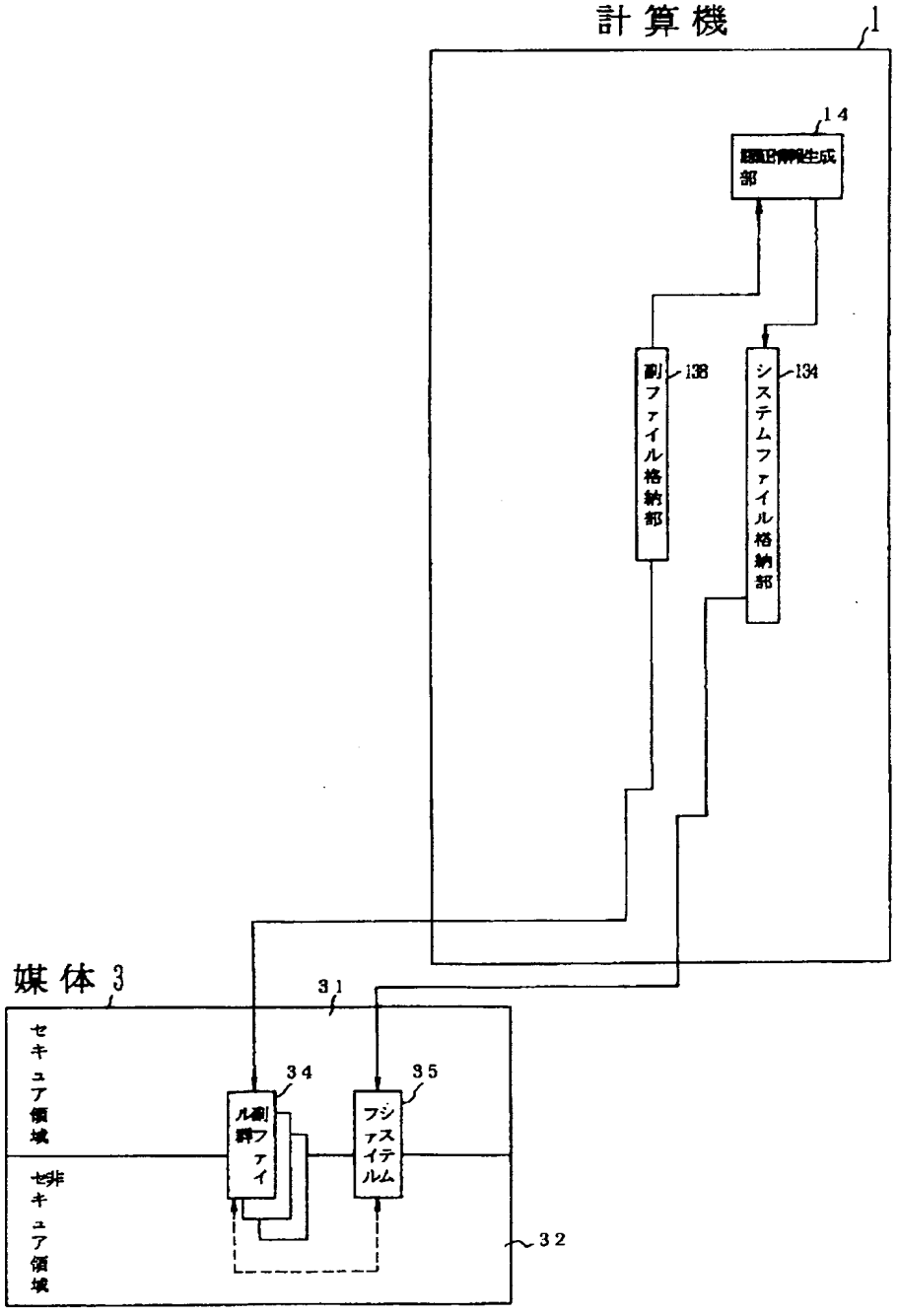
【図４】

本発明の第1の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図



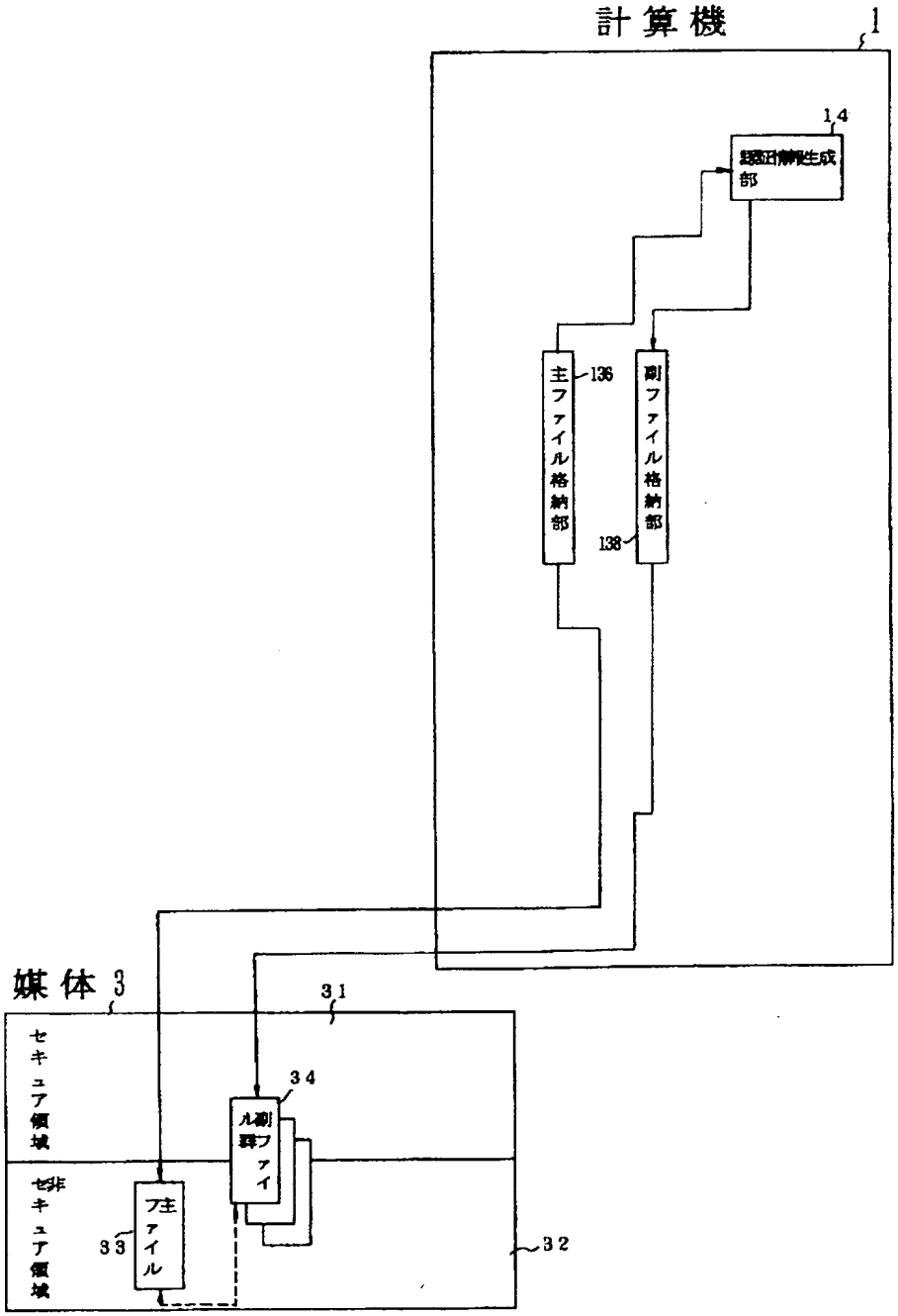
【図６】

本発明の第2の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図



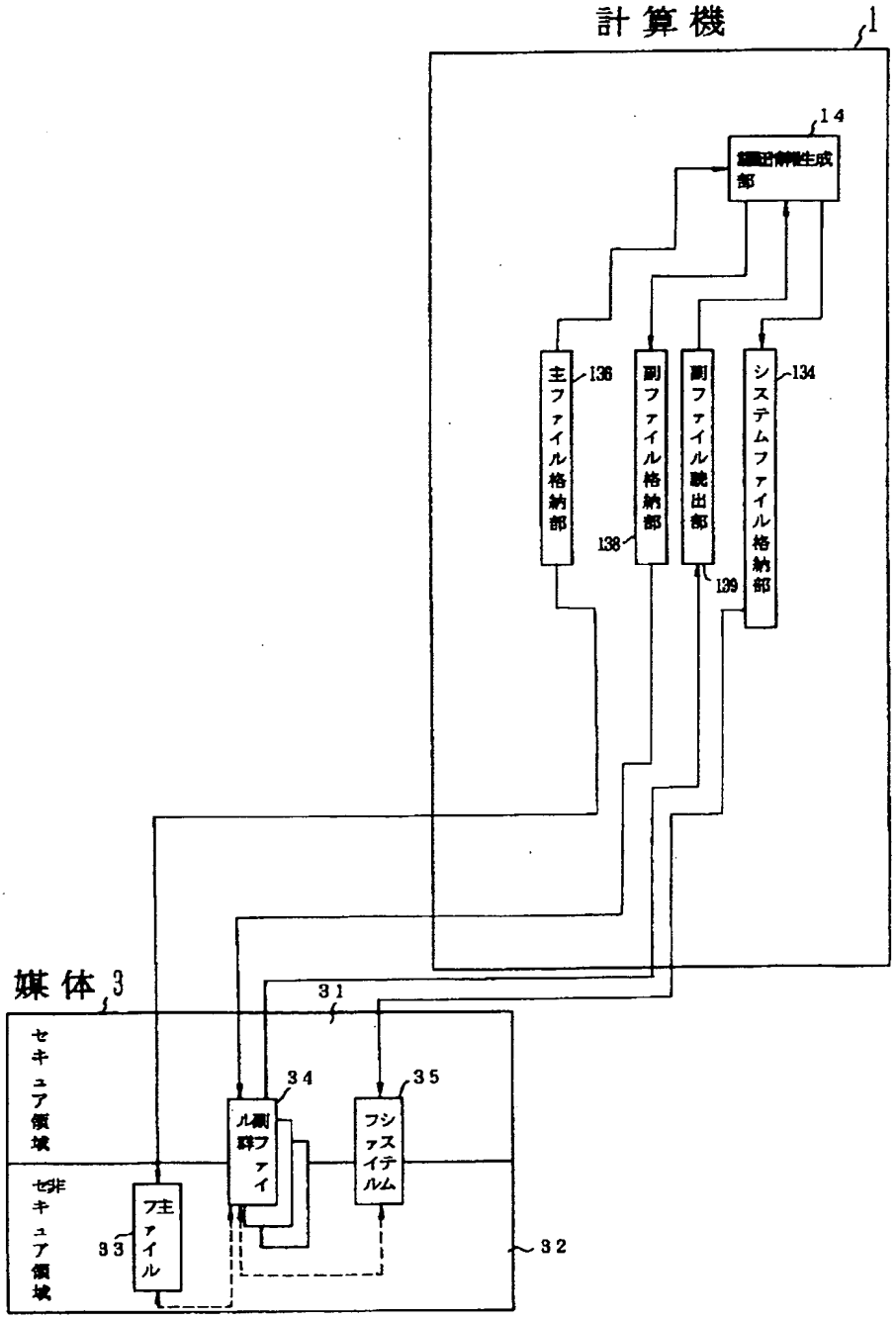
【図８】

本発明の第3の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



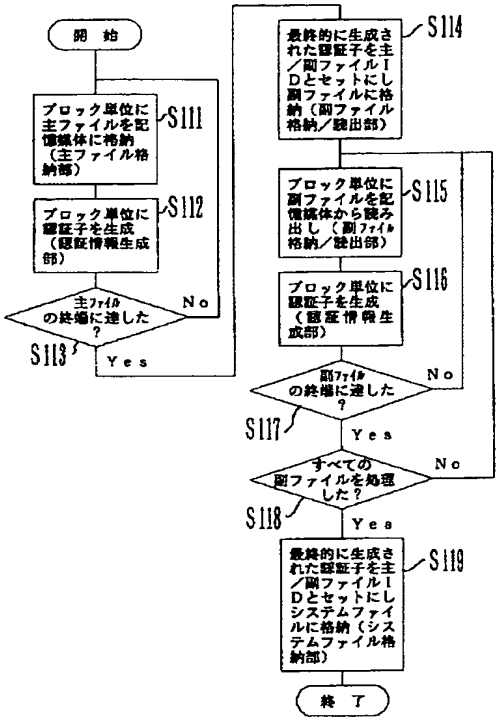
【図１０】

本発明の第4の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



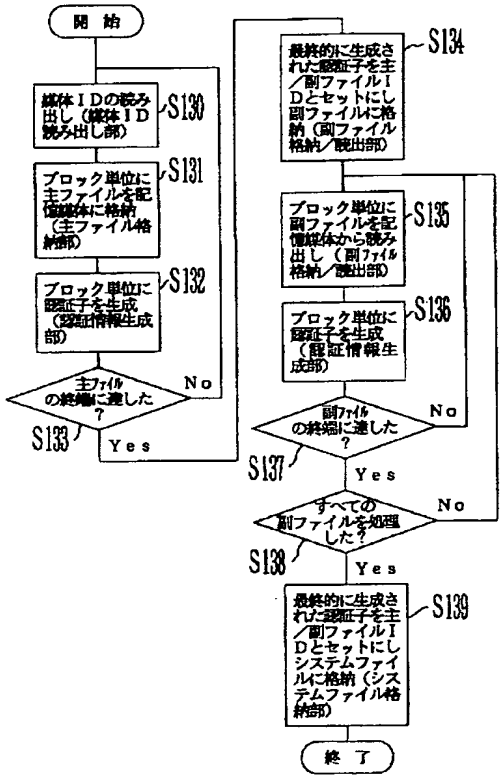
【図１１】

本発明の第４の実施の形態における動作フローチャート



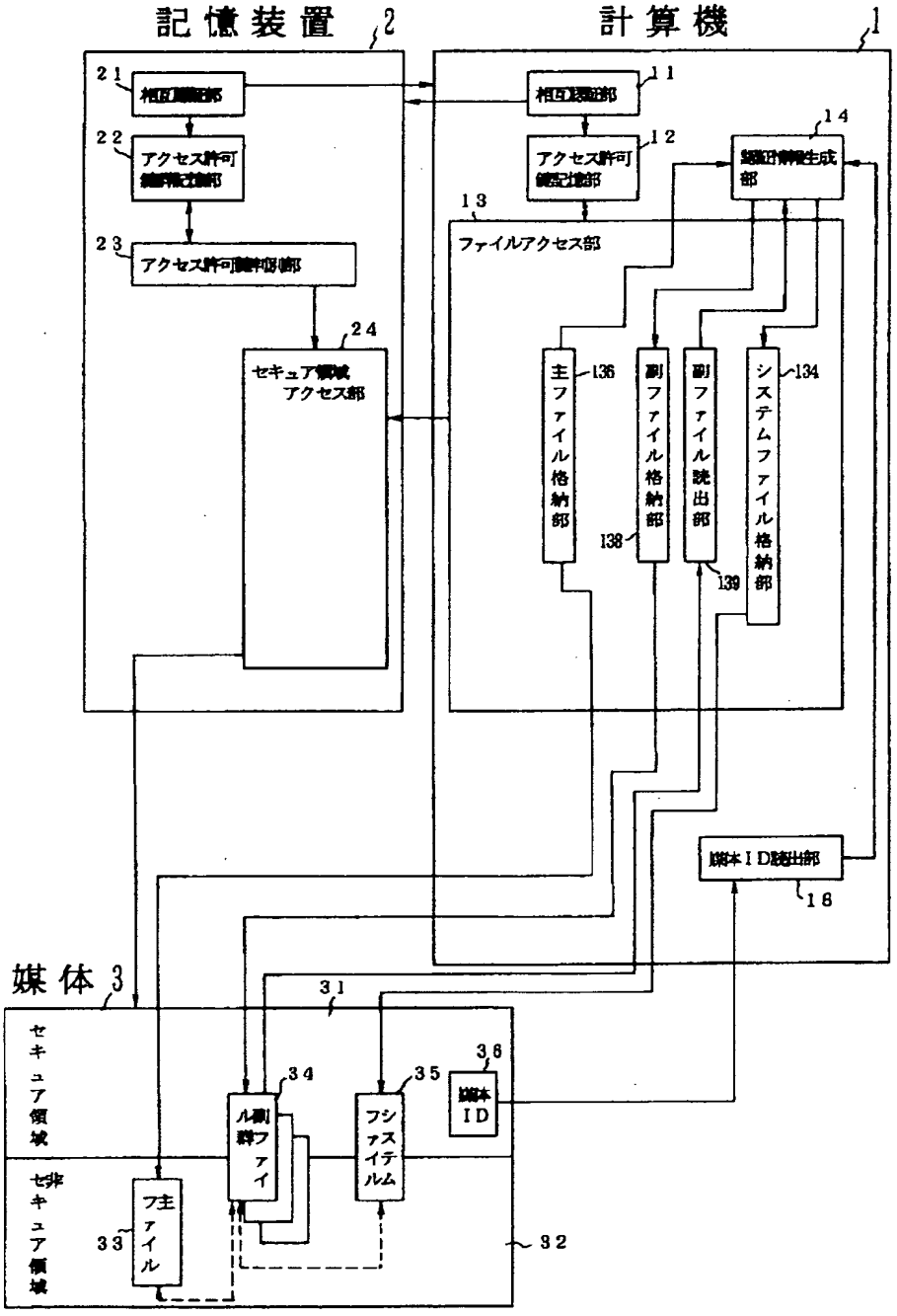
【図１３】

本発明の第５の実施の形態における動作フローチャート



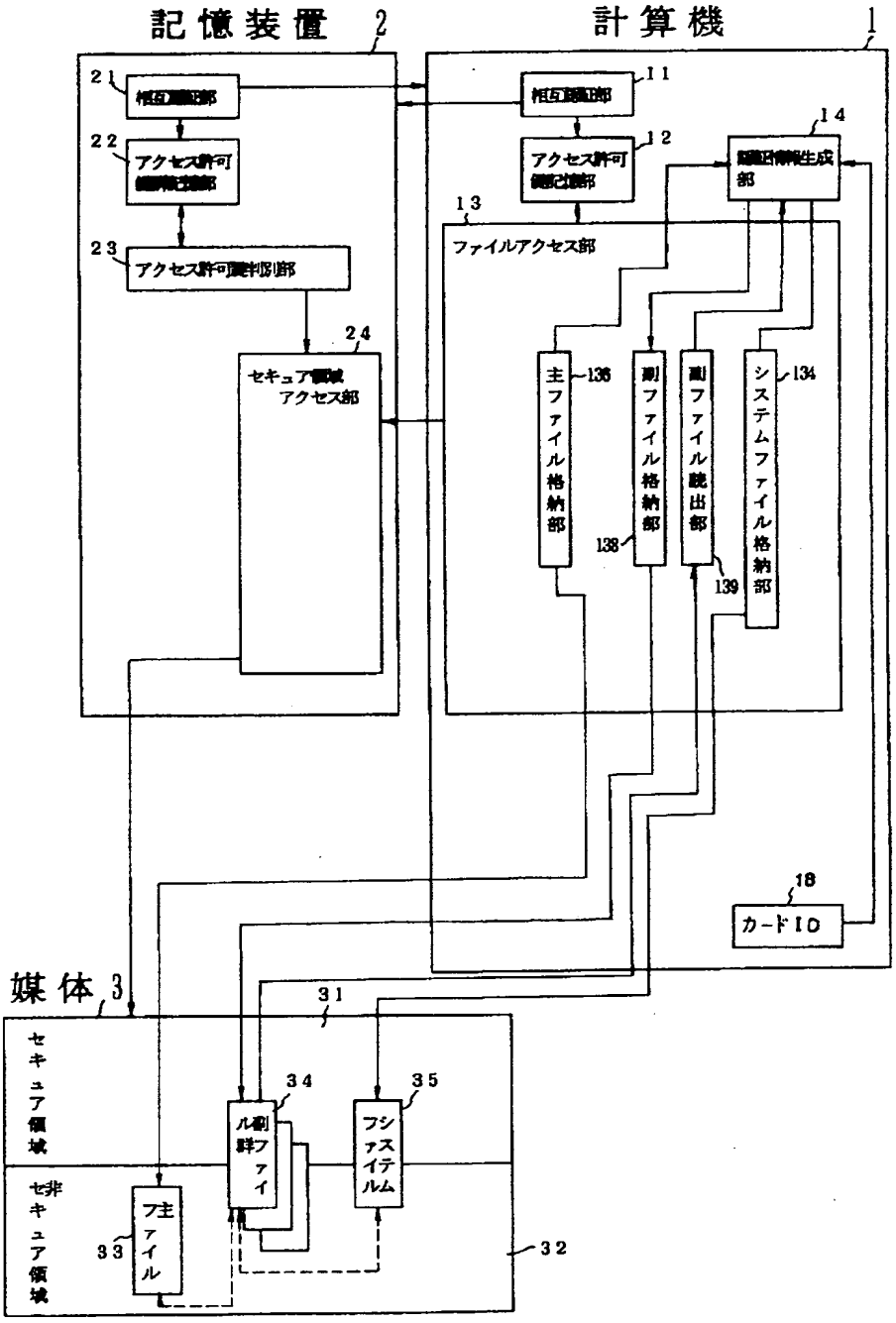
【図１２】

本発明の第5の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



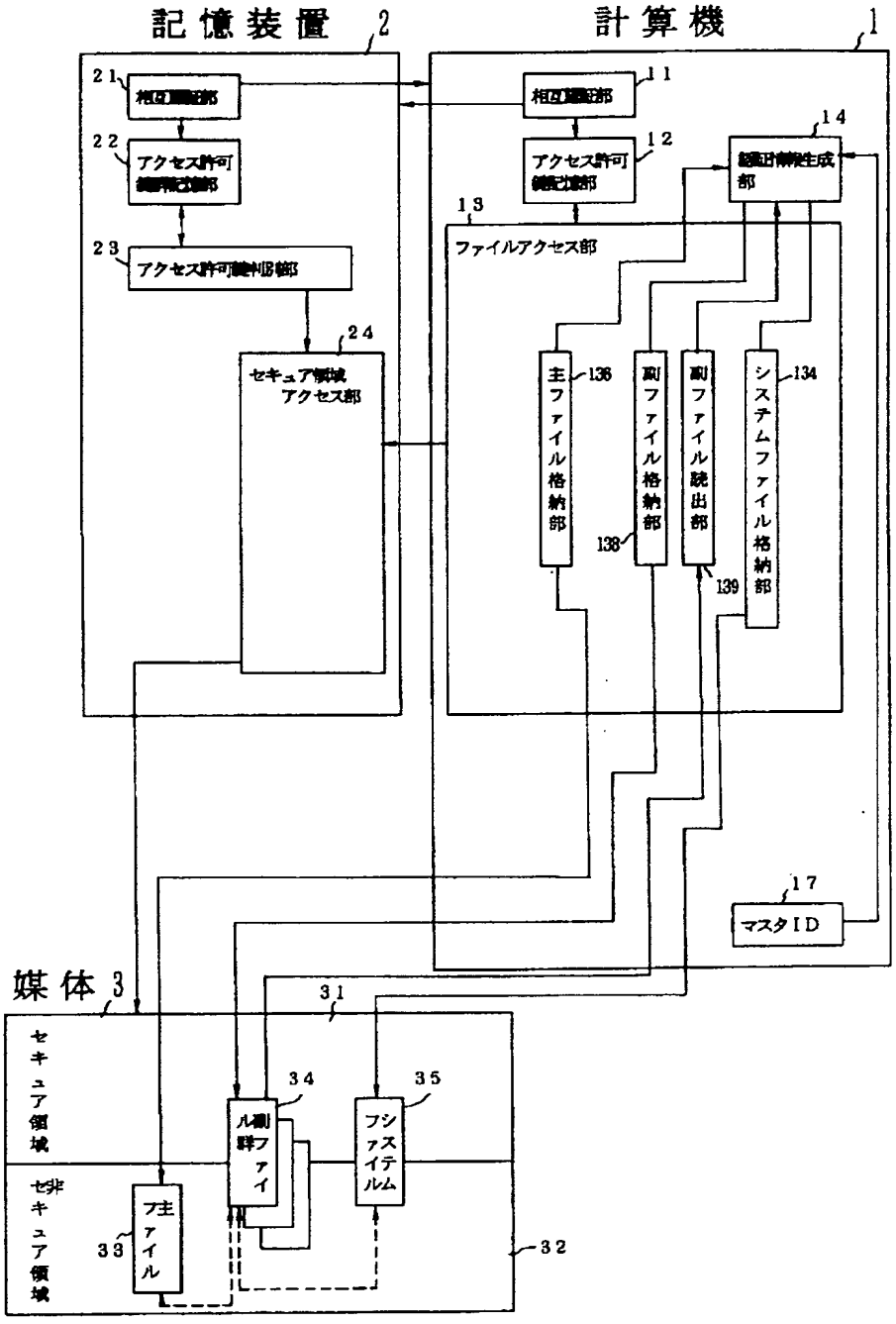
【図１４】

本発明の第6の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



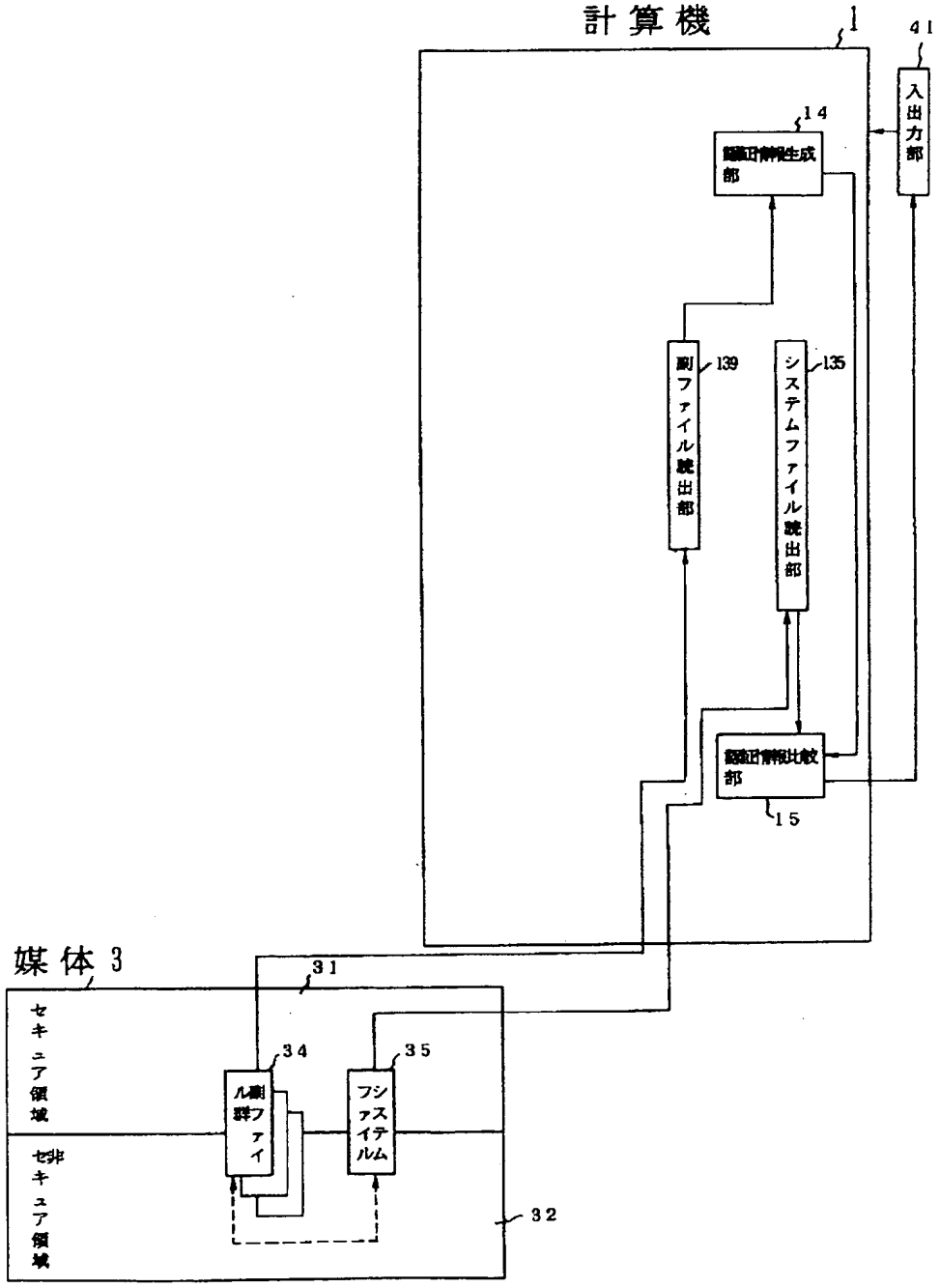
【図１５】

本発明の第７の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図



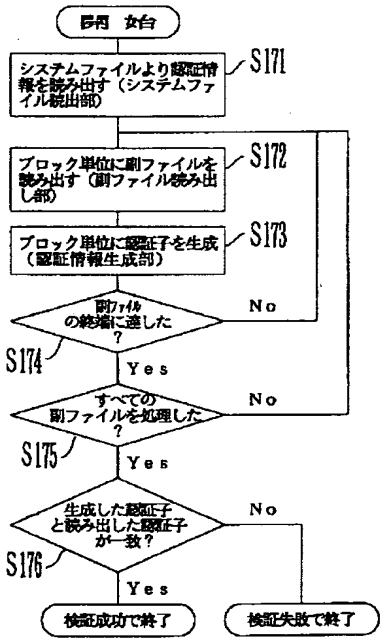
【図16】

本発明の第8の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



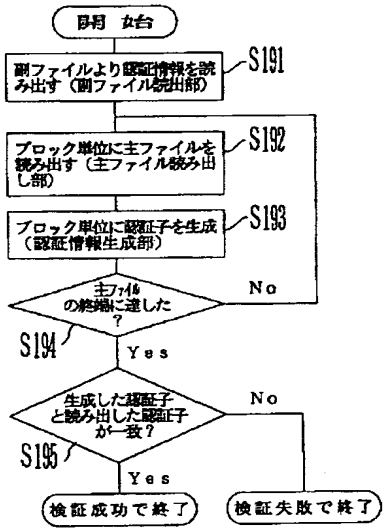
【図１７】

本発明の第８の実施の形態における動作フローチャート



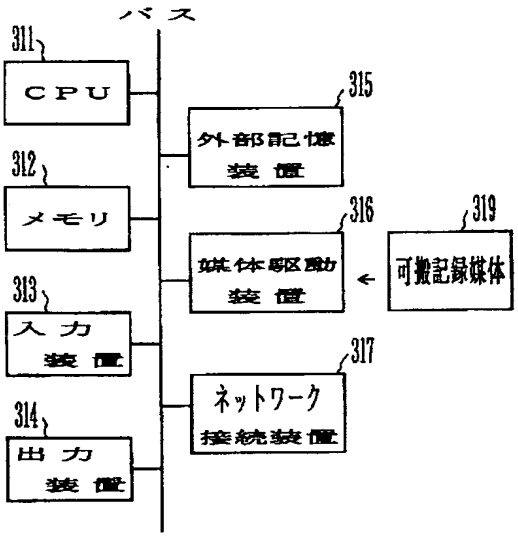
【図１９】

本発明の第９の実施の形態における動作フローチャート



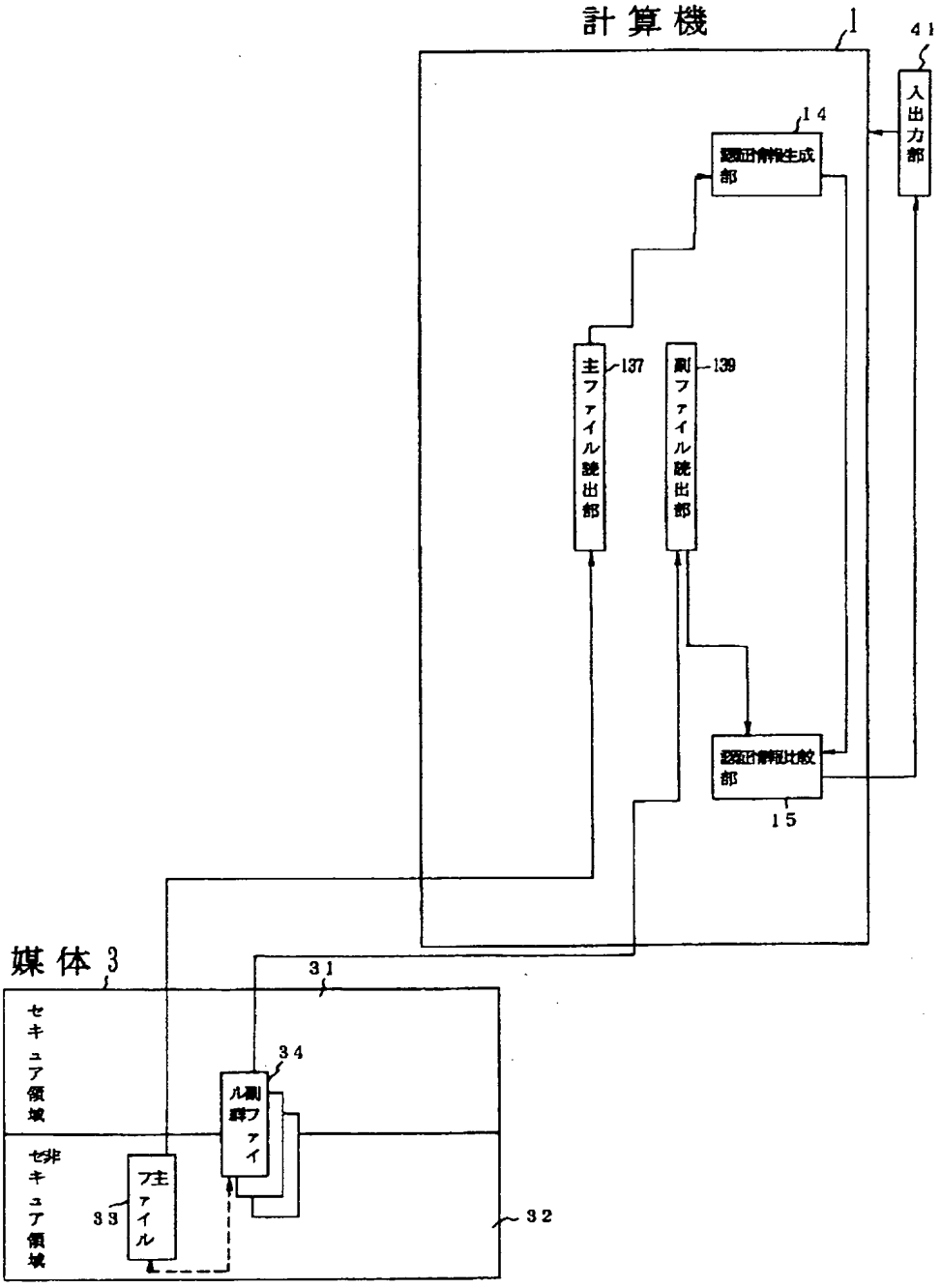
【図３１】

改ざん防止／検出システムの構成図



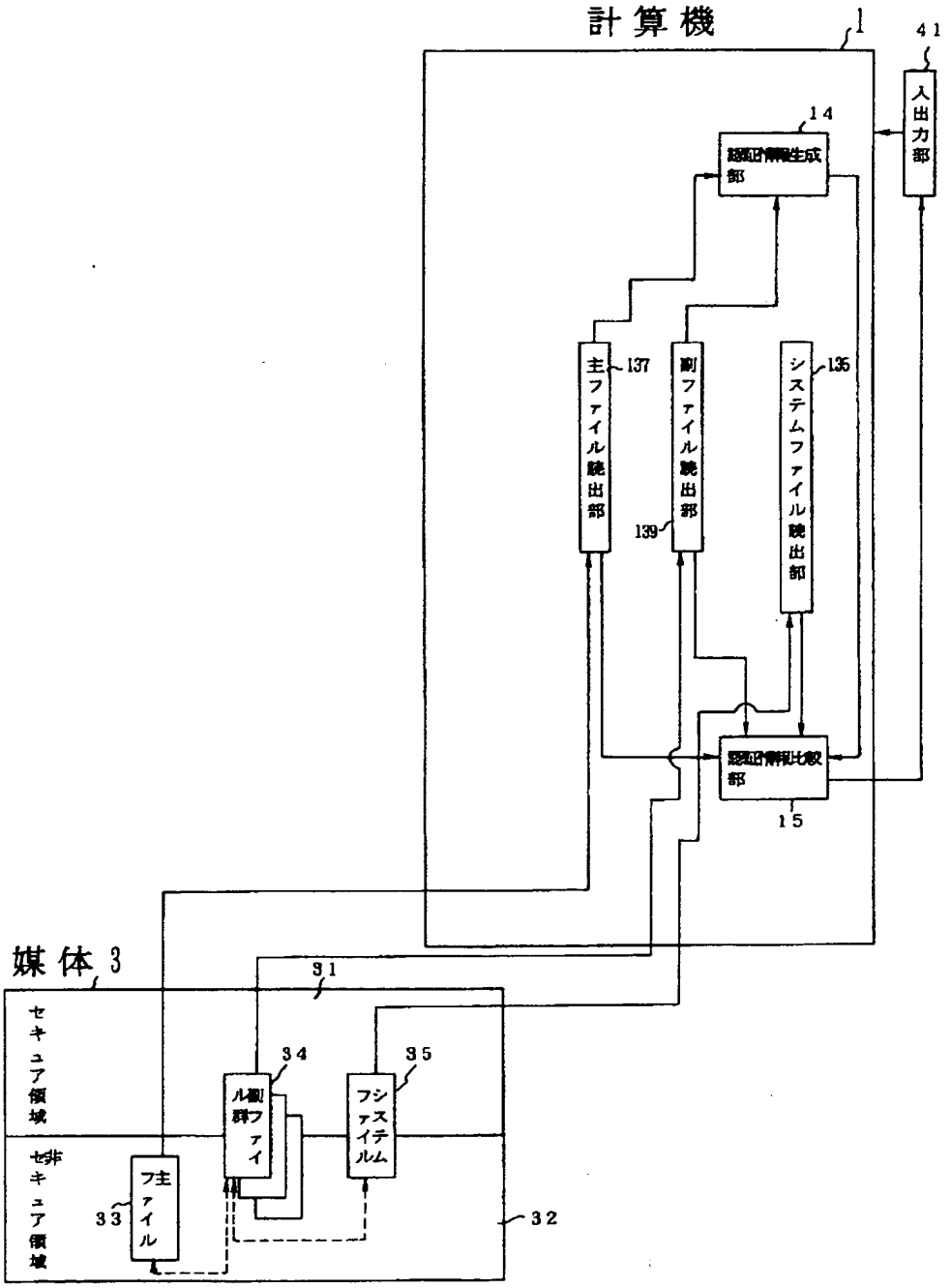
【図１８】

本発明の第9の実施形態における改ざん防止/検出機能を有するファイル管理システムの構成図



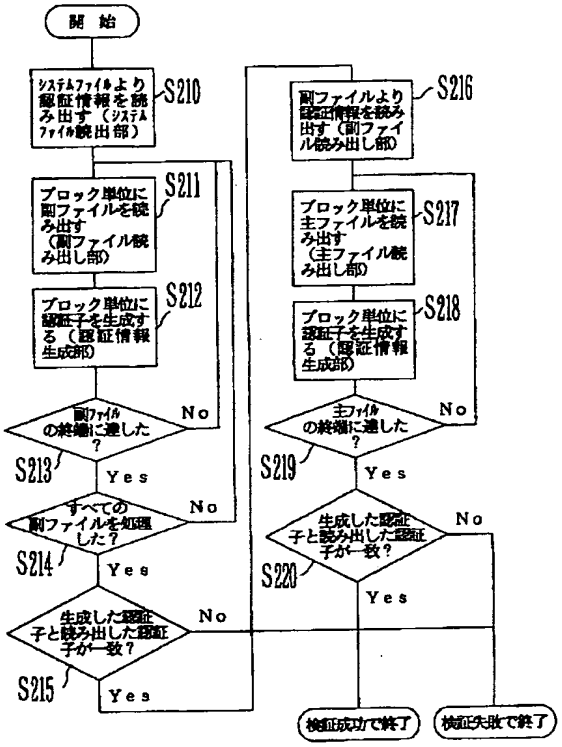
【図２０】

本発明の第10の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図



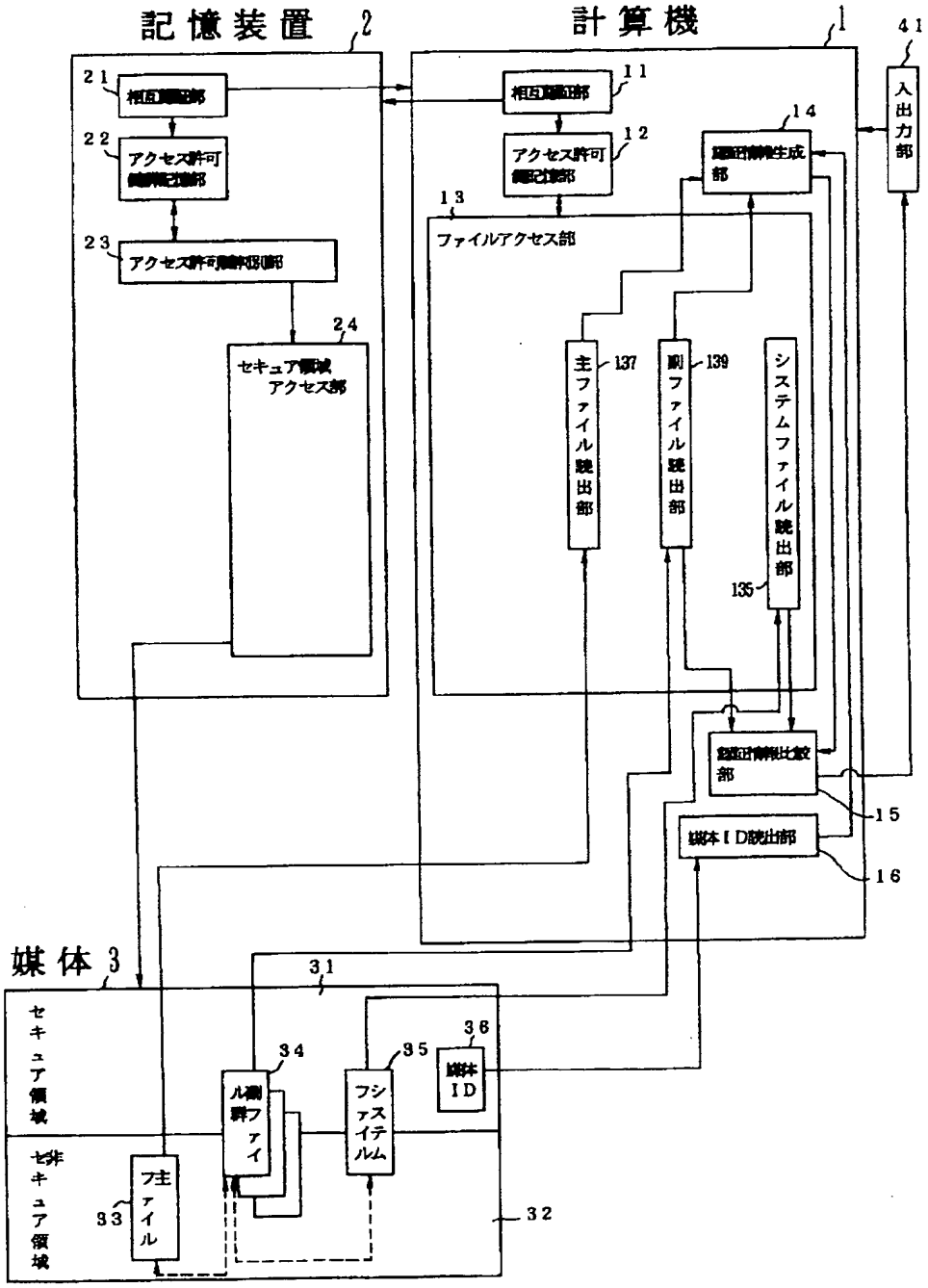
【図２１】

本発明の第10の実施形態における動作フローチャート



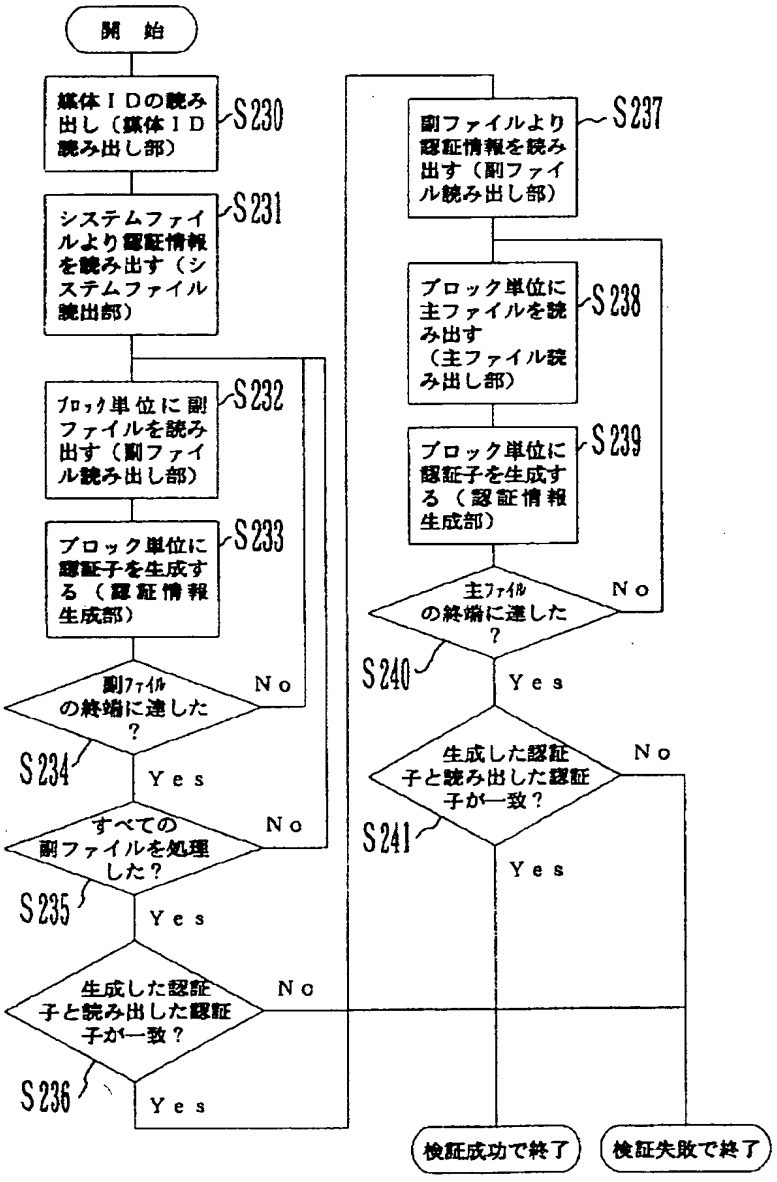
【図２２】

本発明の第11の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



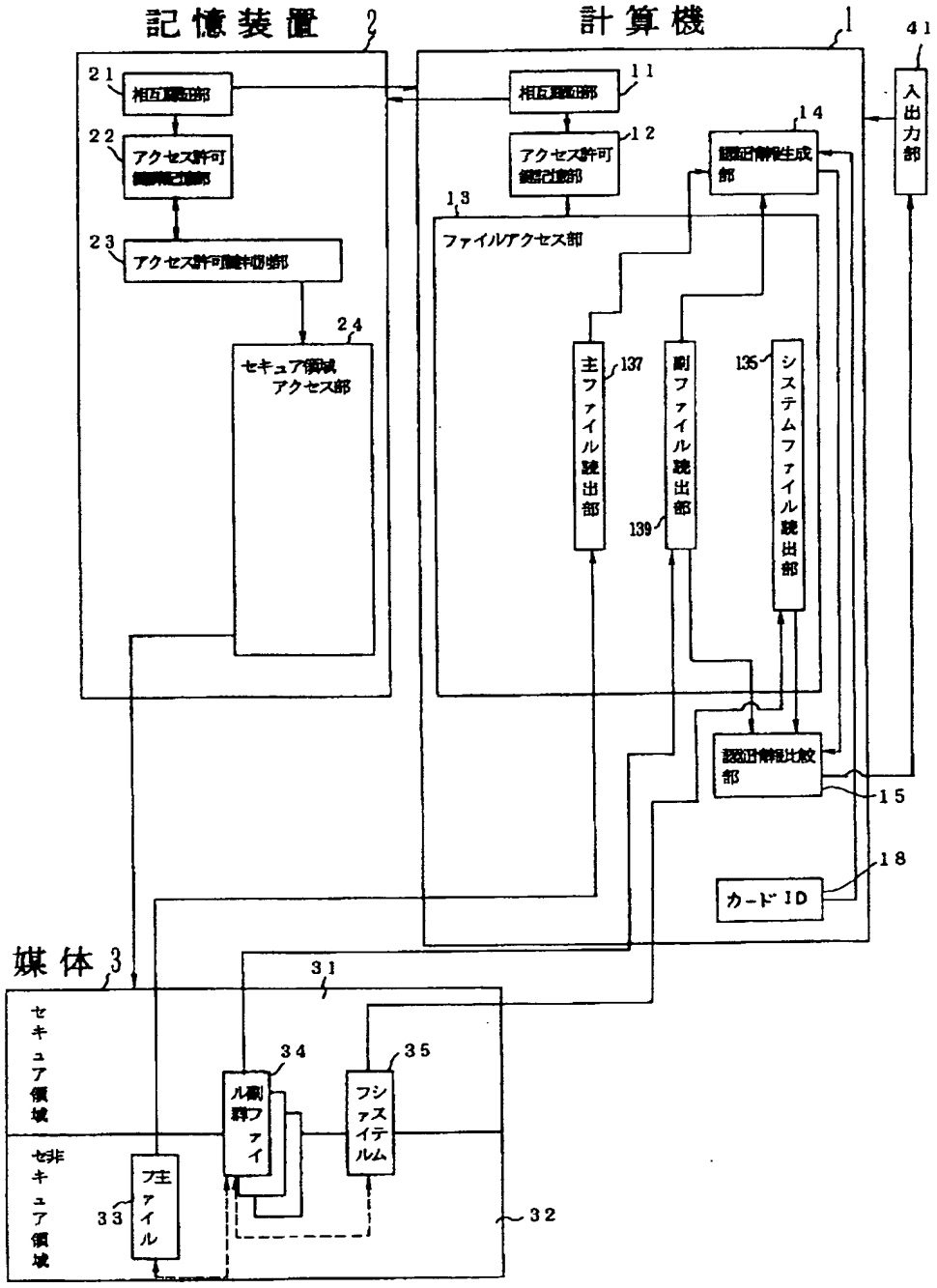
【図２３】

本発明の第11の実施形態における
動作フローチャート



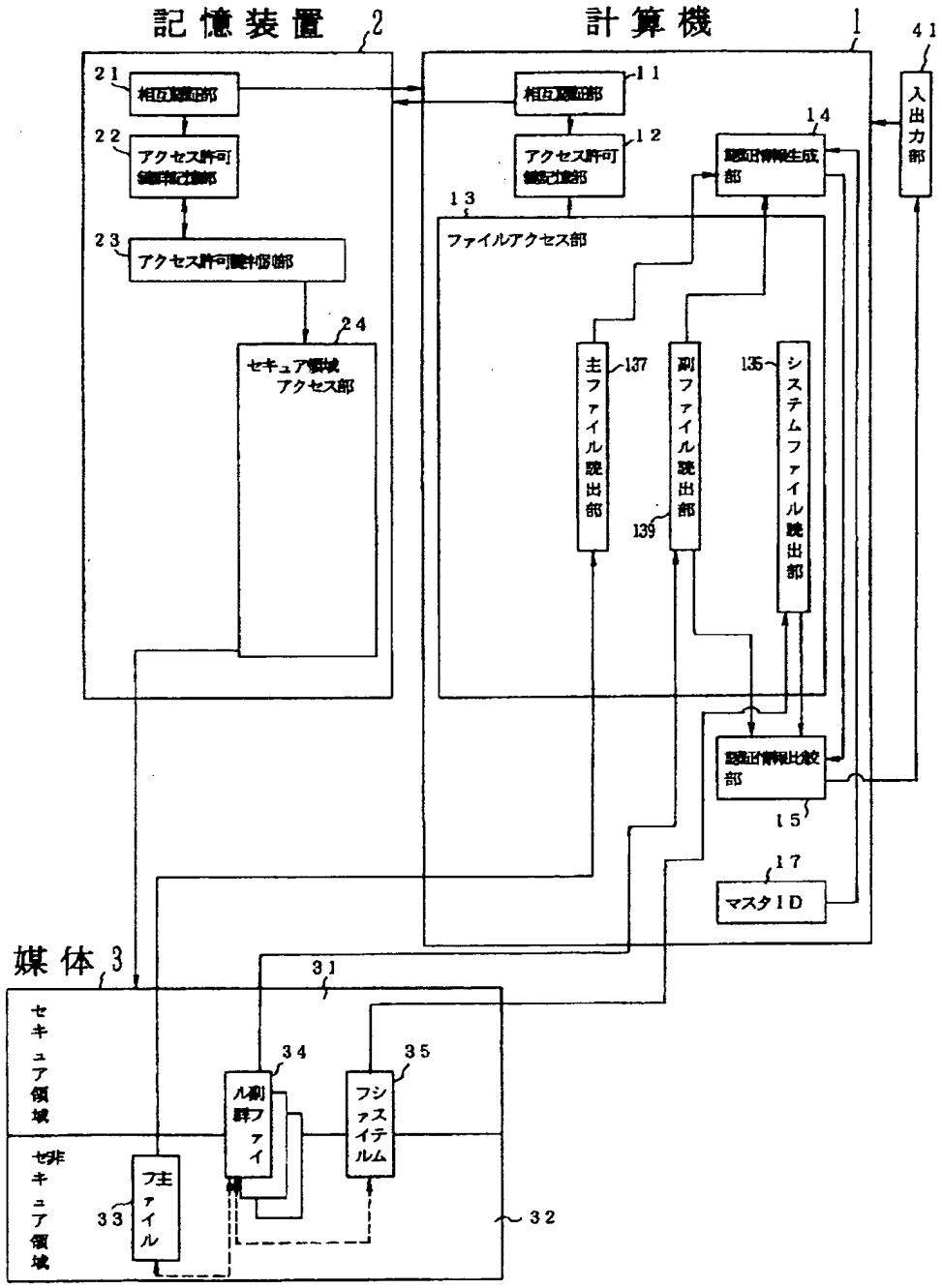
【図２４】

本発明の第12の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



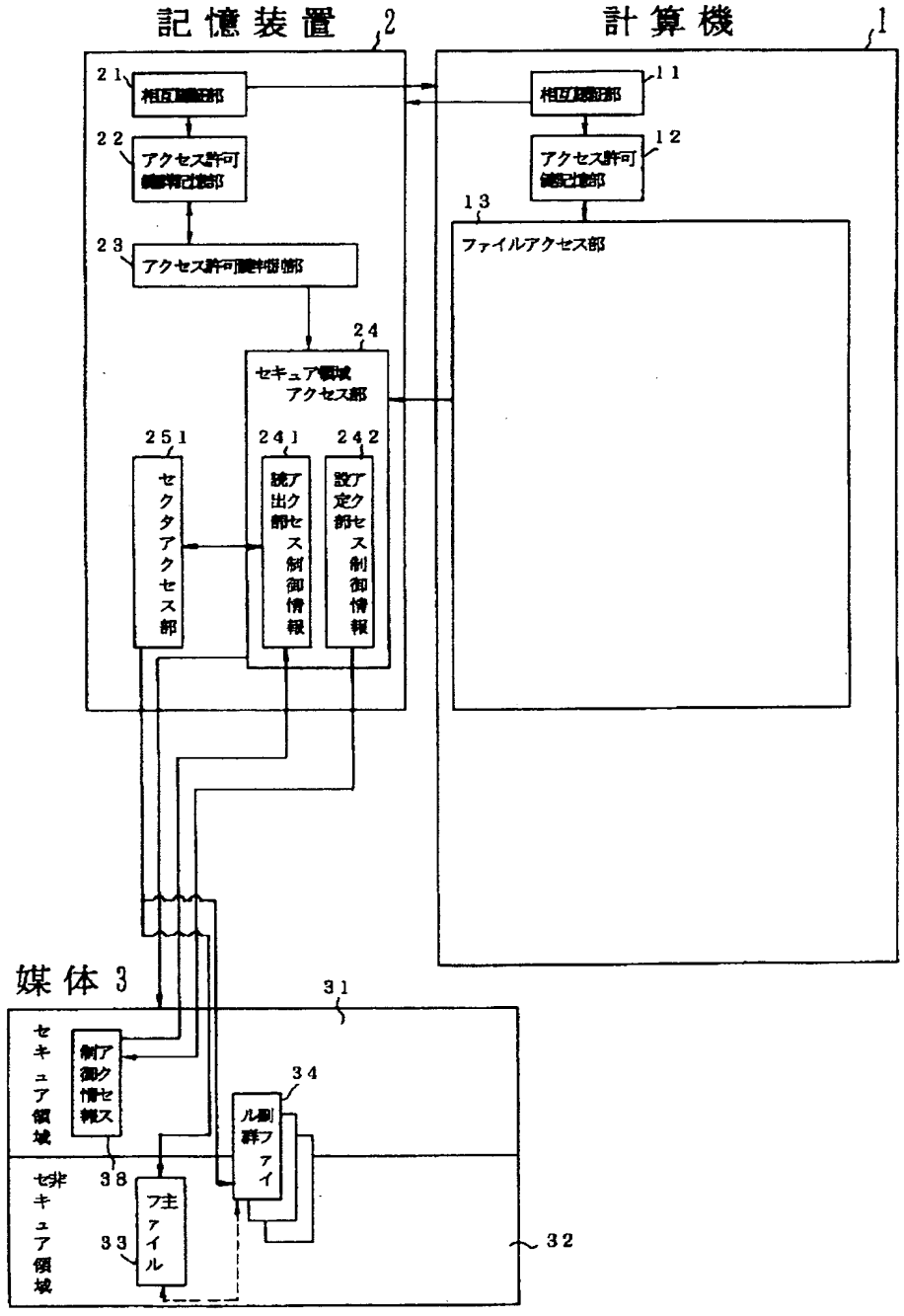
【図２５】

本発明の第13の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



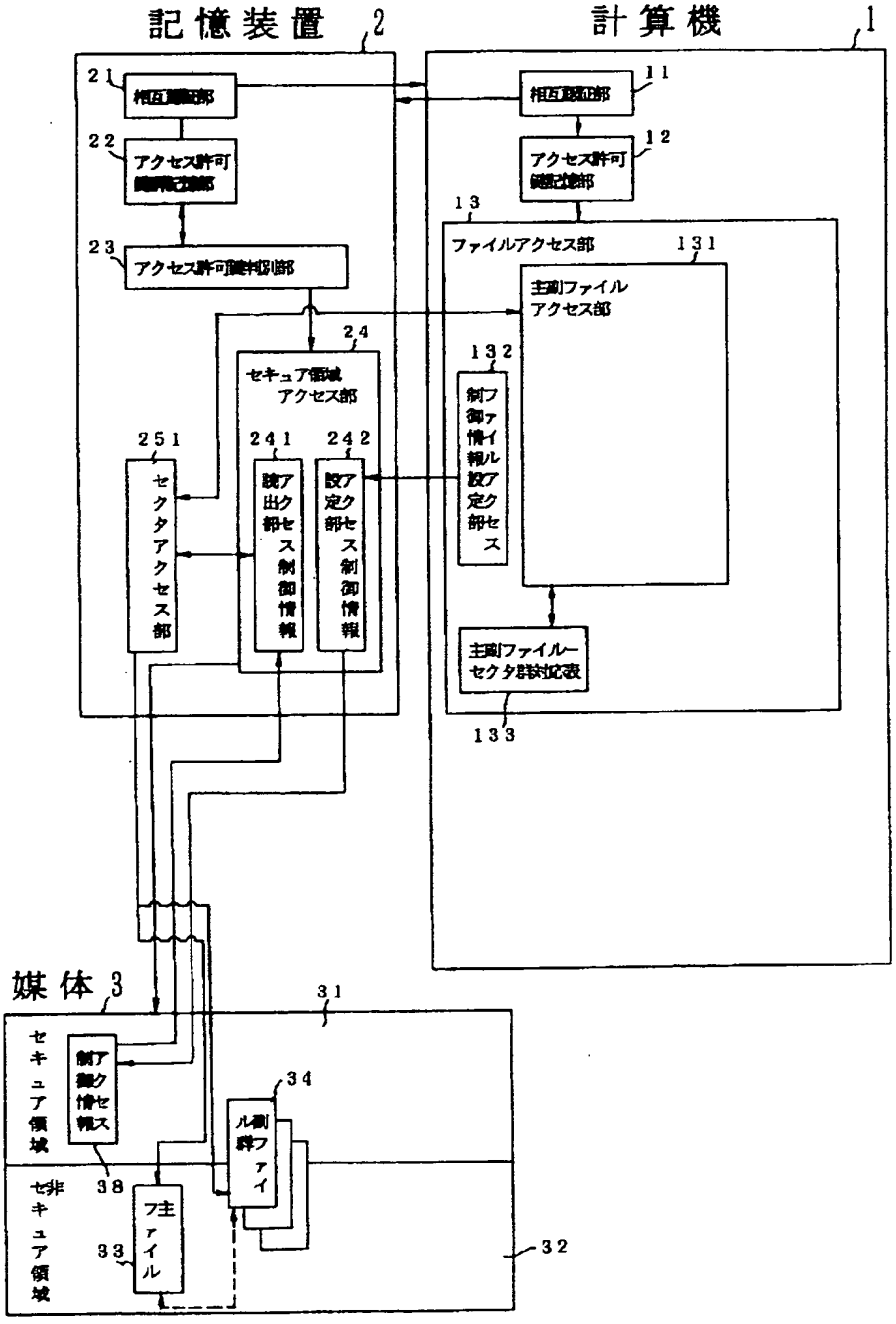
【図２６】

本発明の第14の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



【図２８】

本発明の第15の実施の形態における改ざん防止/検出機能を有するファイル管理システムの構成図



【図３０】

本発明の第16の実施の形態における改ざん防止／検出機能を有するファイル管理システムの構成図